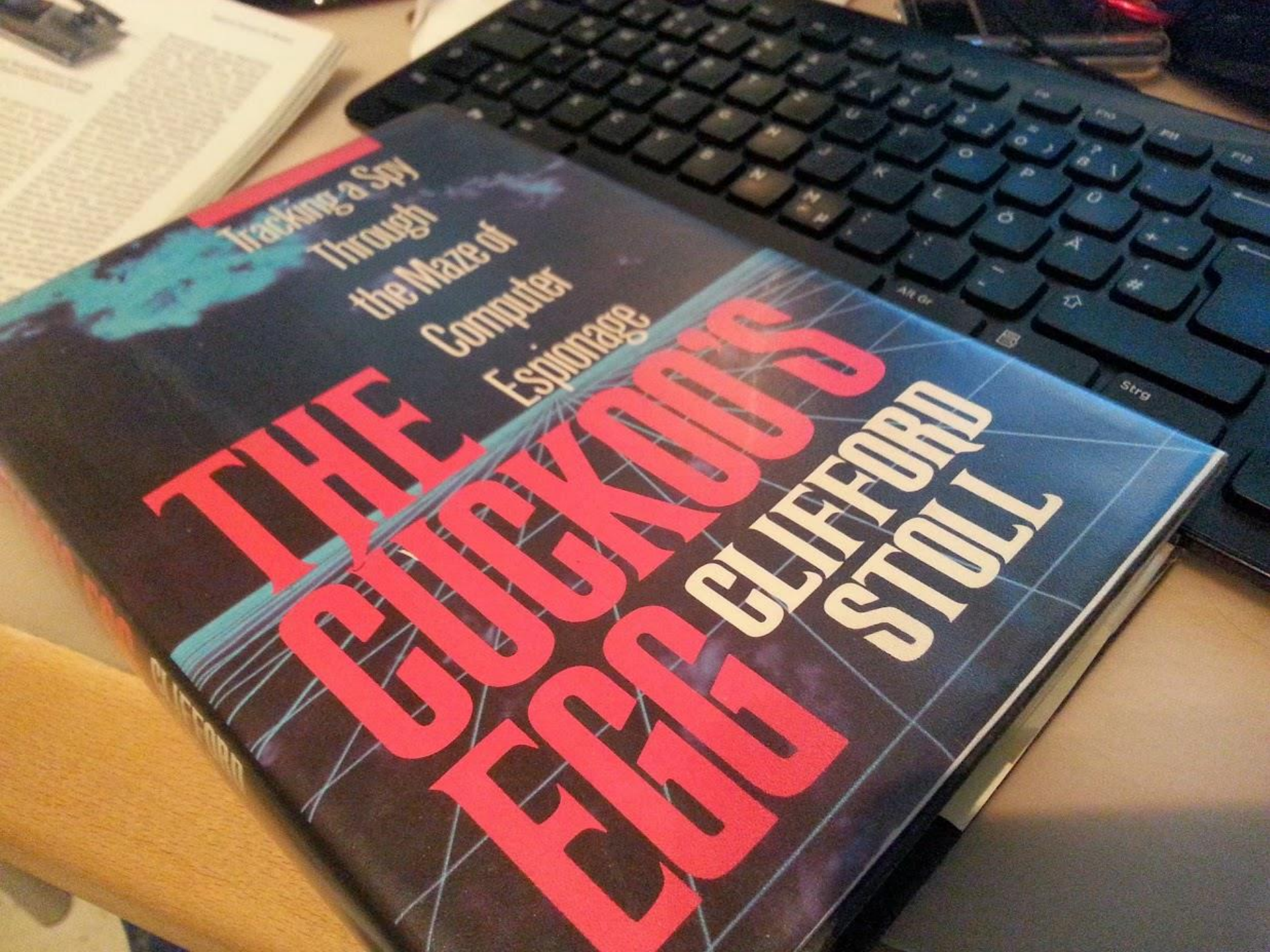
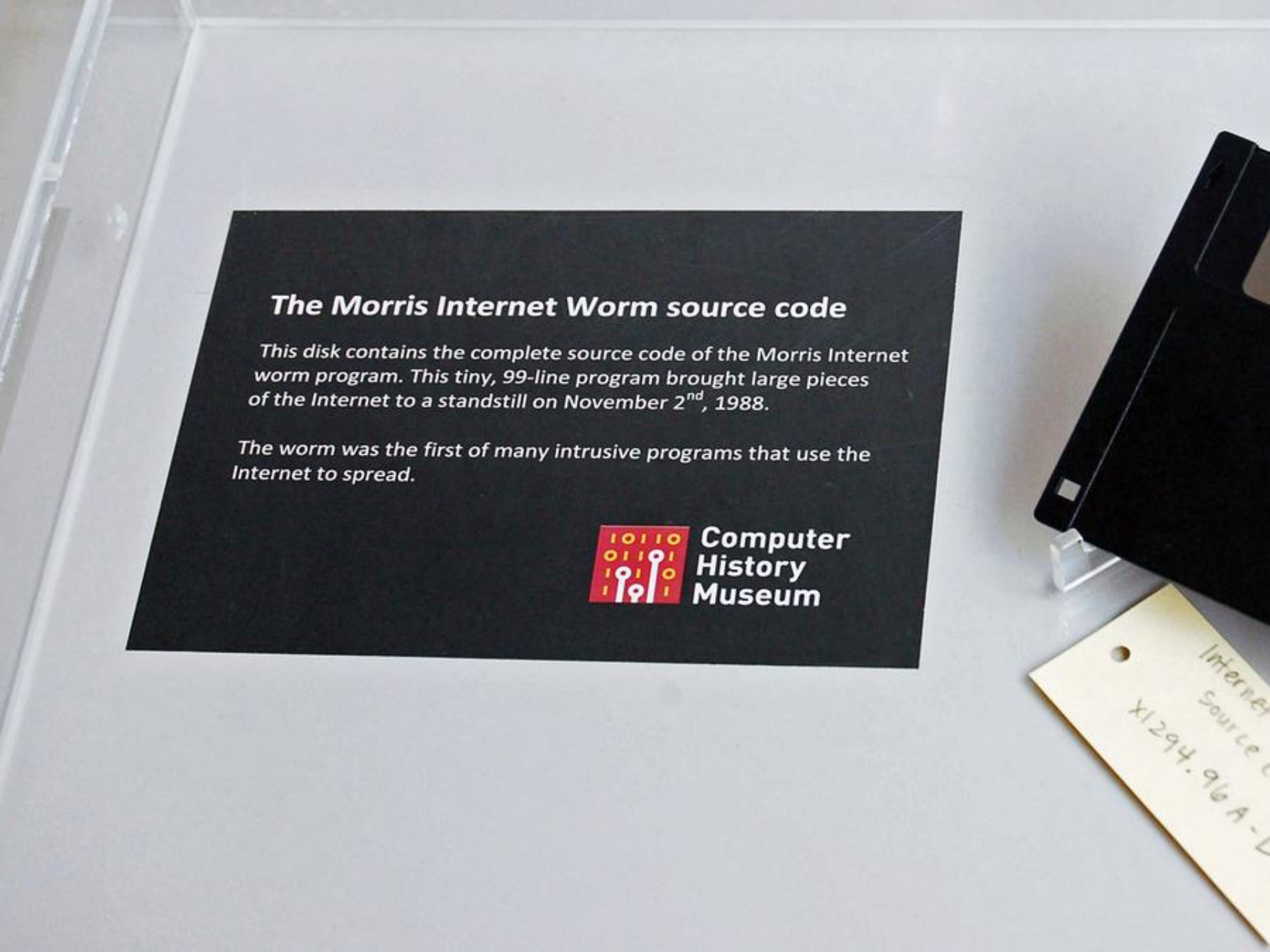
SIKKERHETSMONITORERING: FØR, NÅ, OG I FREMTIDEN

Jan Henrik Schou Straumsheim
mnemonic


Tracking a Spy Through the Maze of Computer Espionage
THE CUCKOO'S EGG
CLIFFORD STOLL


Hunter_


The Morris Internet Worm source code
This disk contains the complete source code of the Morris Internet worm program. This tiny, 99-line program brought large pieces of the Internet to a standstill on November 2nd, 1988.
The worm was the first of many intrusive programs that use the Internet to spread.
Computer History Museum

NORGES STØRSTE MORGENAVIS

Aftenposten

Morgenutgave. Tirsdag 8. november 1988. Uke 45. Nr. 518. 129. årg. Kr. 6,00. Fly/ekspr.: Vest-/Midt-Norge kr. 7,00. Nord-Norge kr. 8,00

Forhindret norsk data-katastrofe

● Han trakk ut kontakten og sparte norske forskningsmiljøer for svarte dataskjermer og millioner i ekstrautgifter. Forskningsleder Pål Spilling i Teledirektoratet (bildet) stanset et amerikansk datavirus før det kom inn i Norge.

● «Viruset» er et innsmuglet program som bruker opp maskinenes datakraft slik at de går i stå. Det har lammet 6000 maskiner i USA. Og det var derfra Spilling fikk beskjeden: — Trekk ut kontakten!

Side 4

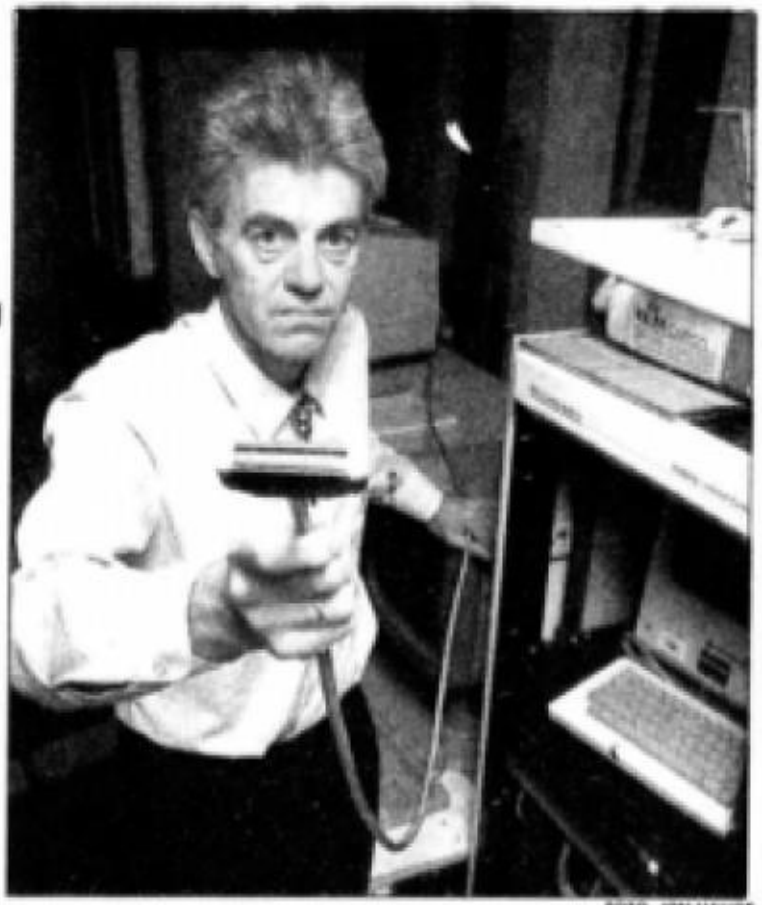


FOTO: JON HAUGE

Software Engineering Institute

Carnegie Mellon

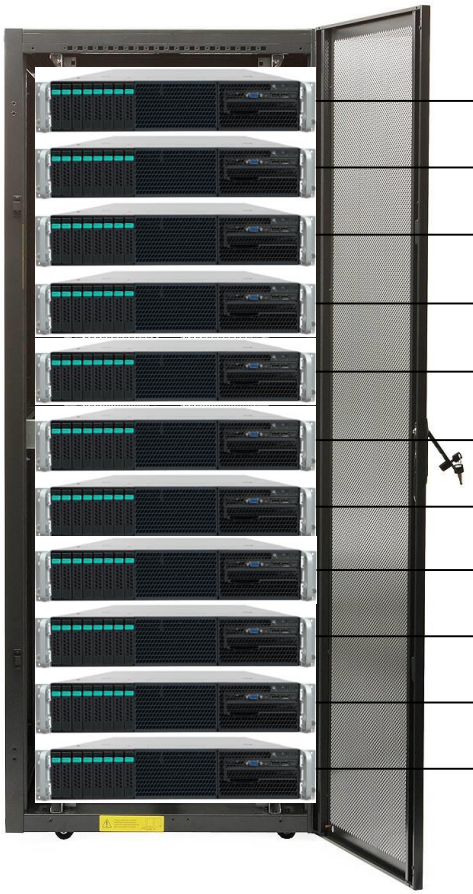
A NETWORK SECURITY MONITOR

L. Todd Heberlein, Gihan V. Dias, Karl N. Levitt, Biswanath Mukherjee, Jeff Wood and *David Wolber*

Division of Computer Science
Department of Electrical Engineering and Computer Science
University of California, Davis
Davis, CA 95616


```
alert tcp $HOME_NET any -> [103.230.84.239] any
(msg:"ET CNC Zeus Tracker Reported CnC Server TCP group 1";
flags:S;
reference:url,doc.emergingthreats.net/bin/view/Main/BotCC;
reference:url,zeustracker.abuse.ch;
threshold: type limit, track by_src, seconds 3600, count 1;
classtype:trojan-activity;
flowbits:set,ET.Evil;
flowbits:set,ET.BotccIP;
sid:2404150;
rev:3611;)
```

mnemonic IDS – Anno 2003

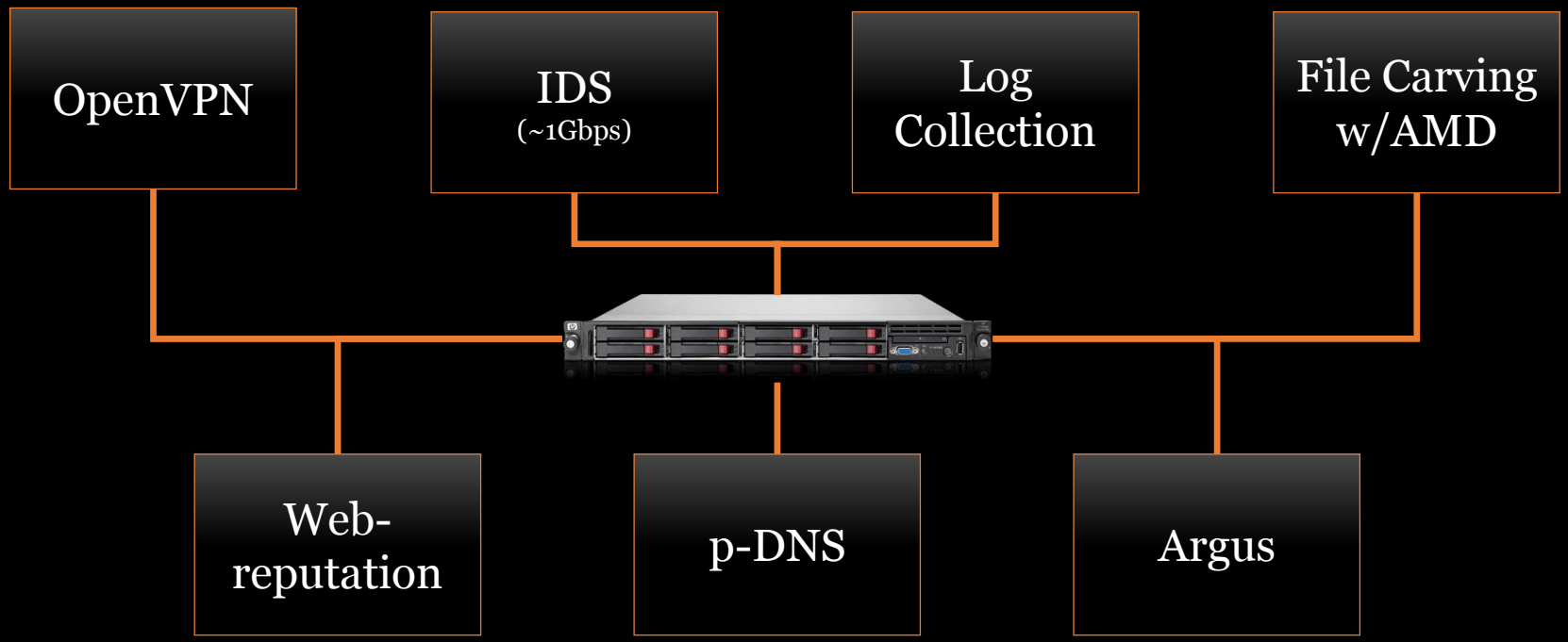


- Snort
- Snort
- ISS
- ISS
- estmon
- estmon
- TopLayer
- Switch
- VPN-GW
- VPN-GW
- Network tap(s)

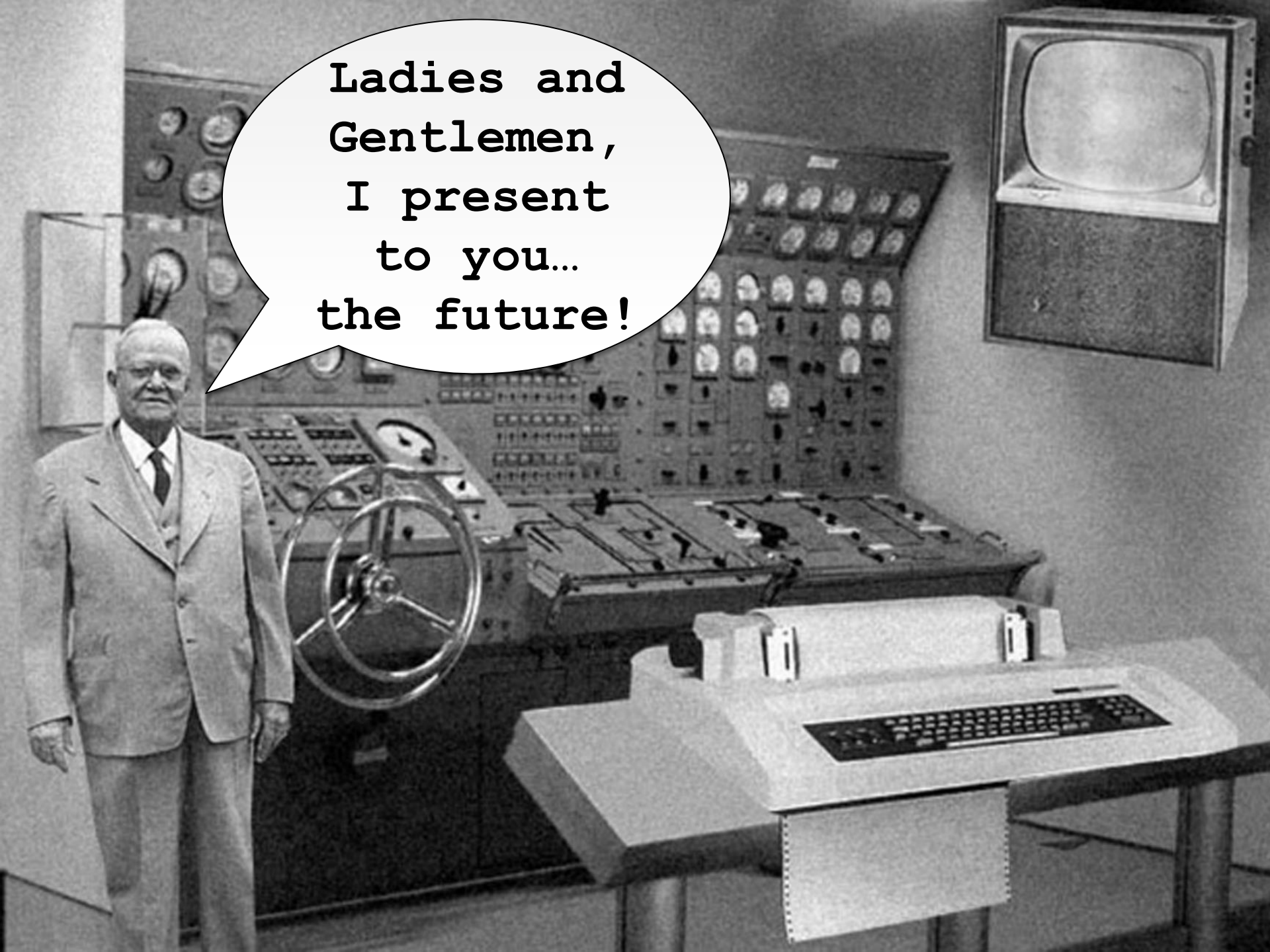
<100 Mbps IDS

mnemonic

mnemonic IDS – Anno 2014



ARGUS
MANAGED DEFENCE


Ladies and Gentlemen, I present to you… the future!

White Paper

Business rationale for de-perimeterisation

KLIENT:

substantiv

Datamaskin som tilbringer ~66% av tiden sin utenfor virksomhetens forsvarsmekanismer.

Spørsmål?

Takk for oppmerksomheten!

Jan Henrik Schou Straumsheim
Sikkerhetskonsulent
mnemonic Security Services
Threat Intelligence
janhenrik@mnemonic.no / 41 52 62 90

mnemonic