Security in Prehistory

Charles Averill - UTD CSG

Historical BG of Computers

- Govt: census, ballistics
- Ind: payroll, inventory
- ARPANET, MULTICS
- Minicomputers, mainframes

User adoption of computers limited before ~1970s, too expensive!

Less adoption -> fewer attackers -> fewer defenses -> more attackers?

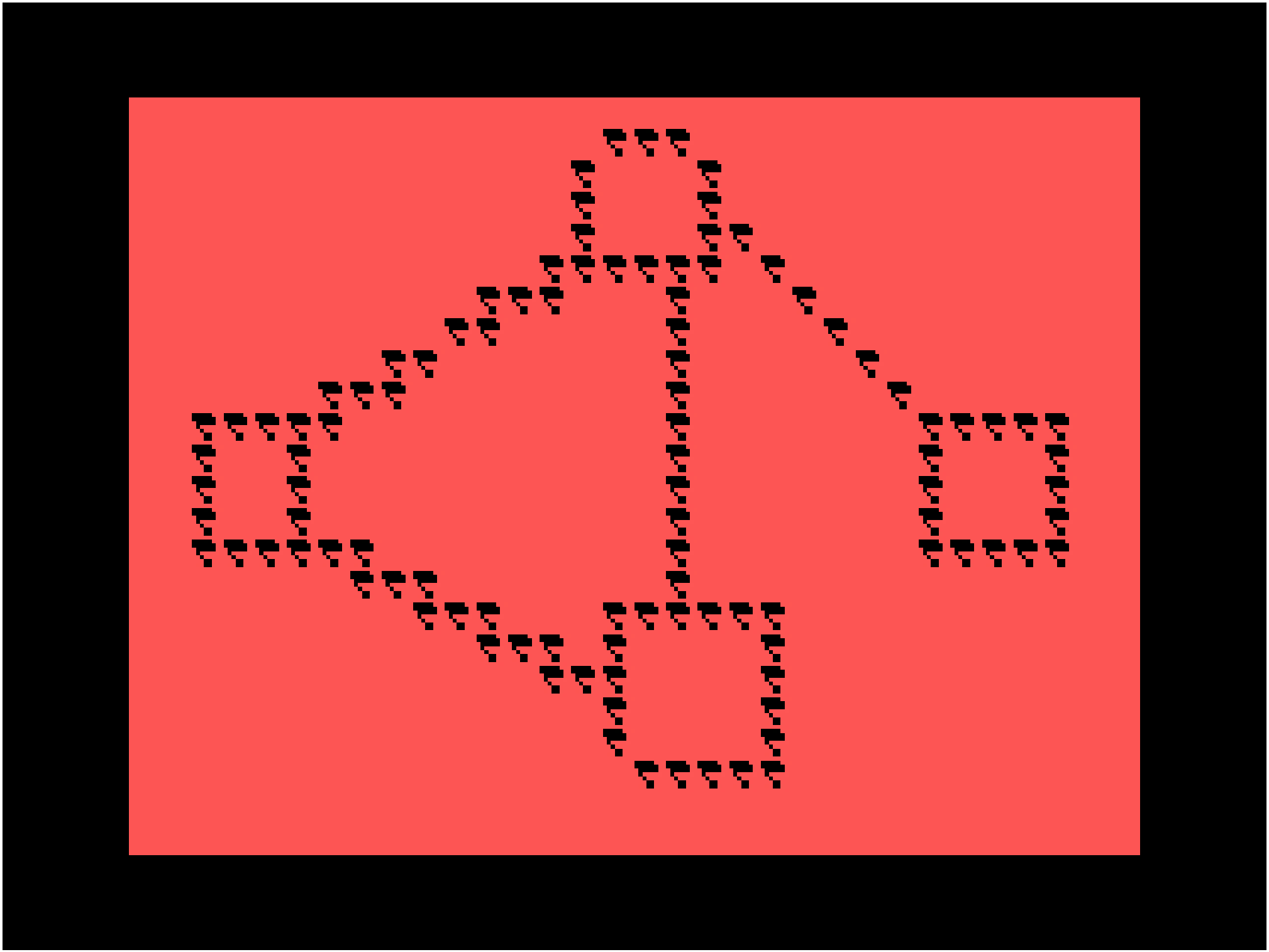
ARPANET - 1969

- Earliest form of internet
- UCLA/SB, SRI ARC, Utah

Trusted members! All nodes were invited universities

Users frequently used default passwords


ARPANET Topology



The 414s - 1982

- Famous early hacking group
- Tgt LANL, ARPANET client!

Found to be teenagers (like in War Games)

$1,500 in damages when breaching Sloan Kettering

Catalyst for CFAA (like War Games!)

Data Encryption Std - 1977

Early symmetric encryption std developed at IBM, NSA

Controversial development, debatable NSA backdoor

56-bit key size, poorly-documented 'S-Boxes'

Key size makes DES weak to brute-force attacks, predicted by Diffie, Hellman

Claimed DES could be brute-forced for $20M in 12 hours, validated in 1998

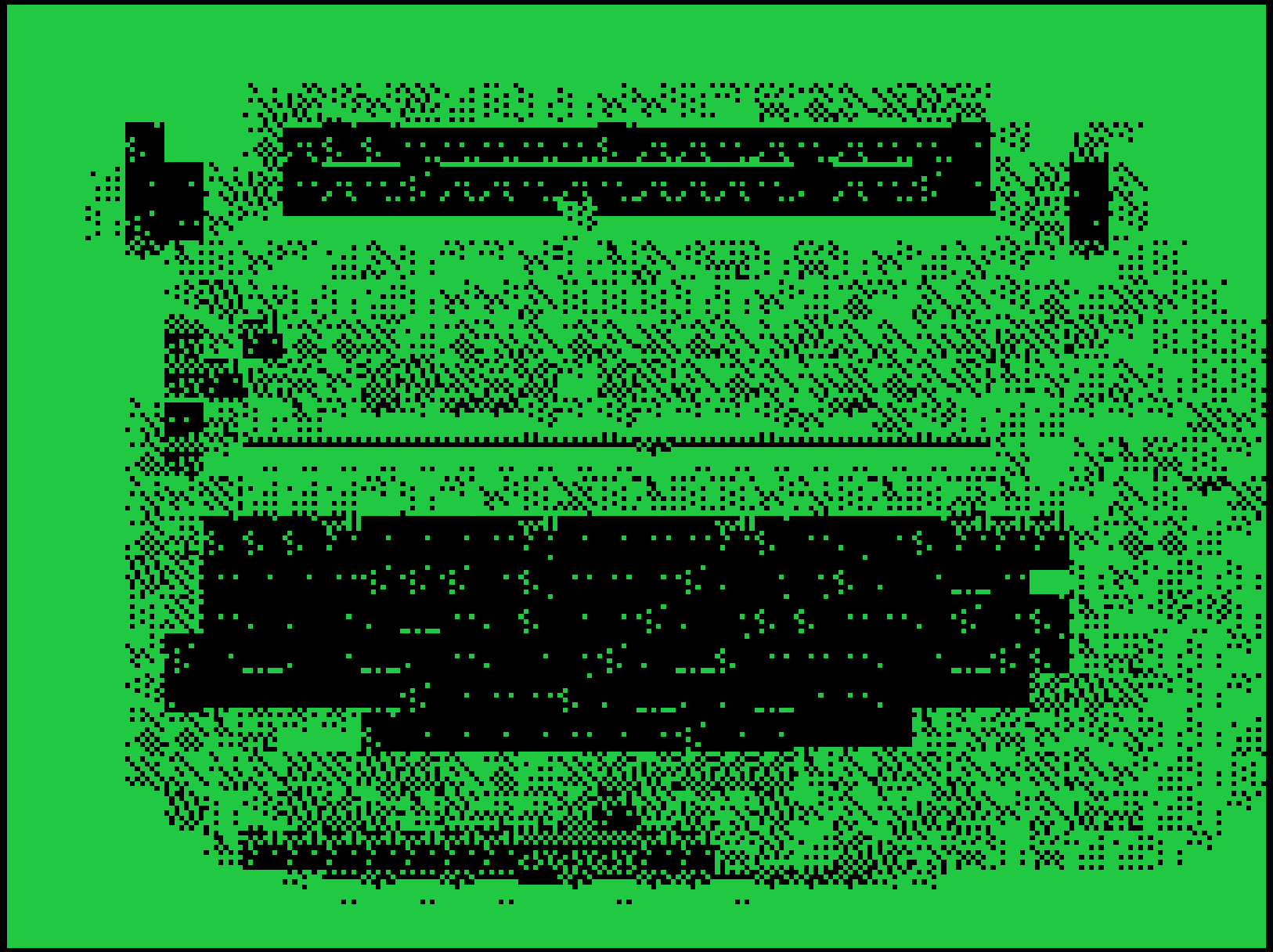
Multics - 1969

Early time-sharing OS from Bell Labs, precursor to Unix
Invented:

Despite focus on security, had multiple notable vulns:

- Weak ring-ring boundaries
- Chosen-plaintext on pw db
- TOCTOU
- Compiler backdoor


IBM Selectric



IBM Selectric Bug - 1976

Used frequently in govt

Types characters by rotating metal ball controlled by magnetic 'transposers'

Soviets replaced a support beam in the chassis to place a bug,

Reads transposer positions with magnemometers

```
  ** DONE **
>
```