## WikipediA

# **ARPANET encryption devices**

The **ARPANET** pioneered the creation of novel **encryption devices** for packet networks in the 1970s and 1980s, and as such were ancestors to today's <u>IPsec</u> architecture, and <u>High Assurance Internet</u> <u>Protocol Encryptor</u> (HAIPE) devices more specifically.

DuPont and Fidler provide a historical perspective of ARPANET encryption devices in the broader evolution of computer networks and cybersecurity.<sup>[1]</sup> They focus primarily on the first such ARPANET device, the Private Line Interface (PLI). That said, the PLI was just the first in a series of devices created during the 1970s and 1980s in ARPANET-related research and development:<sup>[2]</sup>

- Private Line Interface (PLI)
- Black-Crypto-Red (BCR)
- Blacker
- Internet Private Line Interface (IPLI)

#### Contents

Private Line Interface (PLI)

Black-Crypto-Red (BCR)

Blacker

Internet Private Line Interface (IPLI)

References

#### **Private Line Interface (PLI)**

The Private Line Interface (PLI) was the first packet encryptor, sponsored by the <u>Advanced Research Projects</u> <u>Agency</u> and implemented by <u>BBN Technologies</u> as part of the creation of the ARPANET. It was in an early ideation phase by 1973,<sup>[3]</sup> with a stated goal of providing users with the equivalent of a private, leased line through the ARPANET. In that early phase, the PLI was envisioned to provide two distinct capabilities: transferring a continuous bit steam over the ARPANET, and possibly encrypting the bit stream while it was within the ARPANET.

As design progressed, it evolved into a packet encryption device, which was approved starting in 1975 by the <u>National Security Agency</u> for limited deployment on the ARPANET, to protect classified data as it passed through the network.<sup>[4]</sup> Each PLI device incorporated a <u>KG-34</u> encryption device, and as a result was a manually keyed system.<sup>[5]</sup>

# Black-Crypto-Red (BCR)



Diagram of a Private Line Interface (PLI) for the ARPANET, BBN Report 2816, April 1974. Black-Crypto-Red (BCR) was an experimental, end-to-end, network packet encryption system developed in a working prototype form by BBN and the Collins Radio division of <u>Rockwell</u> between 1975-1980. BCR was the first network security system to support <u>TCP/IP</u> traffic for IPv3, and it incorporated the first <u>Data</u> <u>Encryption Standard</u> (DES) chips that were validated by the U.S. National Bureau of Standards (now called NIST).<sup>[6]</sup> It provided automated, KDC-based key management and access control (as later adopted by Kerberos and Blacker),<sup>[7]</sup> and supported IP header bypass.<sup>[8]</sup>

## Blacker

The first Blacker program began in the late 1970s, with a follow-on eventually producing fielded devices in the late 1980s.<sup>[9]</sup> It was sponsored by the National Security Agency as a very high assurance (A1), multi-level security system, and developed by SDC (software) and Burroughs (hardware), and after their merger, by the resultant company Unisys.<sup>[10]</sup>

# **Internet Private Line Interface (IPLI)**

The Internet Private Line Interface (IPLI) was created by BBN as a successor to the PLI. It was updated to use TCP/IP (IPv4) and newer COMSEC technology (KG-84), but still manually keyed.<sup>[11]</sup> They were intended for use in the <u>Defense Data Network</u> and also in DARPA Low-Cost Packet Radios in the <u>SURAN</u> project.

#### References

- 1. "Edge Cryptography and the Codevelopment of Computer Networks and Cybersecurity", by Quinn DuPont, Bradley Fidler, *IEEE Annals of Computing*, vol. 38, Oct.-Dec. 2016, pages 55-73.
- 2. "Re: Network Layer Encryption History and Prior Art" (http://www.sandelman.ca/ipsec/1996/06/ msg00050.html), email by Steve Kent on the ipsec mailing list, Wed, 19 Jun 1996 10:59:39 +0100
- 3. "Interface Messages Processors for the ARPA Network" (https://apps.dtic.mil/dtic/tr/fulltext/u2/7 <u>63734.pdf)</u>, Quarterly Technical Report No. 2, by Frank E. Heart, BBN Report 2580, <u>BBN</u> Technologies, pages 10-13.
- 4. Kent, ibid.
- 5. "Interface a Private Line Interface (PLI) to an IMP and a Host to a PLI", in *Specifications for the Interconnection of a Host and an IMP*, BBN Report No. 1822, Appendix H, January 1976.
- 6. Internet Security Glossary, Version 2, RFC 4949, August 2007.
- 7. Kent, ibid.
- 8. *Trust in Cyberspace*, National Academies Press, 1999, page 301.
- DARPA Technical Accomplishments: An Historical Review of DARPA Projects (https://apps.dti c.mil/dtic/tr/fulltext/u2/a239925.pdf), vol. 1, by Sidney G. Reed, Richard H. Van Atta, and Seymore J. Deitchman, IDA Paper P-2192, 1990, pages 20-18 to 20-20.
- 10. Kent, ibid.
- 11. Kent, ibid.

#### Retrieved from "https://en.wikipedia.org/w/index.php?title=ARPANET\_encryption\_devices&oldid=1008457342"

This page was last edited on 23 February 2021, at 11:30 (UTC).

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia

Foundation, Inc., a non-profit organization.