CrypTech

Trusted Open Source Security Hardware

Internet users seeking to encrypt data and preserve their privacy have a wide variety of open source tools to choose from. But not every tool has open source alternatives, particularly security hardware, a small market dominated by a handful of vendors who offer exclusively closed source and proprietary products. That's where CrypTech comes in. CrypTech, an independent international development effort, was founded to create trusted, inexpensive, open source, hardware cryptographic engines. It supports the Internet community by providing an open and auditable alternative to existing crypto devices.

What if your encryption wasn't truly private?

One of the main reasons to encrypt stored data or network transmissions is to keep them private: to ensure that no one can snoop or steal the data. This type of encryption has become a pervasive best practice. Hard drives, websites, email—today, virtually everything is encrypted.

But what if encryption tools don't work as advertised? What if encryption isn't giving us the privacy we want? These are the questions that have occupied many IT professionals in recent years, since secret documents were released that revealed the pervasive monitoring of our communications and the compromise of some network and security products. What do you think? Are our tools and software free from corruption? Are our algorithms secure? Have our security appliances been tampered with?

Diversity, openness, and transparency help solve corruption and tampering.

Our most trusted security algorithms are open and transparent; the best minds in the world help to ensure that they have no flaws. And a; continual, open process of evaluation and testing is underway for every important algorithm. When flaws are discovered, they are quickly reported.

The problem occurs when these algorithms are translated into hardware and software. When security software and hardware have bugs, everything is at risk. Closed source and proprietary tools can have bugs, as well as Trojan horses (hidden, intentionally planted weaknesses) that are ready to be exploited. Open source software and transparent development processes offer Internet users alternative ways to secure their communications and maintain their privacy. When you use diverse tools, you reduce the risk of a security failure.

Building open source hardware is expensive.

Writing open source software tools requires only a small investment: a personal computer and little else. Building open source hardware is another matter. Developing prototype boards, burning code into specialized chips, and creating special-purpose circuits require a substantial investment.

CrypTech brings the ideas and philosophies of open source software and transparent development to hardware cryptography. CrypTech's hardware designs are free for everyone to use, including individuals, organizations, and hardware manufacturers. They also may be used as the basis for new cryptographic products.

The CrypTech team is geographically diverse, its members reside in Germany, Japan, Russia, Sweden, and the United States. With a proposed budget of nearly USD $1,000,000 a year, CrypTech has laid out a three-year plan to provide tested, open source reference designs for cryptographic hardware, and is protecting these designs with licenses that enable use and reuse.

CrypTech needs your help.

The money for CrypTech comes from the Internet community. With only half of the budget funded, CrypTech seeks the support of the Internet community. **How much is privacy and security worth to you?** To learan more about how you can help support CrypTech, see https://cryptech.is/funding.

CrypTech
https://cryptech.is