Silicon Safe: Company Overview

Silicon:SAFE

PASSWORD PROTECT
SOLVING THE PROBLEM OF BULK IDENTITY THEFT

About Silicon Safe

Silicon Safe Ltd is a UK company developing simple hardware technologies to prevent bulk identity theft via cyber-attack. Silicon Safe was founded in April 2013 to create a unique solution to the increasing problem of bulk password theft, and has since extended its designs to secure biometric data, credit card information and secrets such as launch codes and private certificates. Silicon Safe is now beginning customer trials of its first data protection product, Password Protect.

Silicon Safe has filed patents relating to its technologies in the United Kingdom and the United States, and filed under the international filing convention. It has registered offices in Cambridge, UK at St. John's Innovation Centre, and a development centre at BT's Adastral Park.

Technology: The No-Read Appliance

The underlying concept behind Silicon Safe is breathtakingly simple: hardware that allows secrets to be stored and verified, but never retrieved. With Silicon Safe's patent-pending technology, secrets are isolated at the hardware level – they can be stored and checked for accuracy, but it is electrically impossible to steal them.

This unique approach eliminates all traditional security weaknesses with secret storage and can be delivered as a service, integrated into cloud infrastructure, or packaged as an appliance in datacentres. It is easily integrated with existing identity stores, applications and e-commerce sites.

DATA THEFT HIGHLIGHTS

> Adobe 2013 38 million active passwords	**> Sony Playstation Network** 2010 70M passwords, 12M credit cards
> eBay 2014 145 million passwords	**> Facebook** 2012 45 million passwords

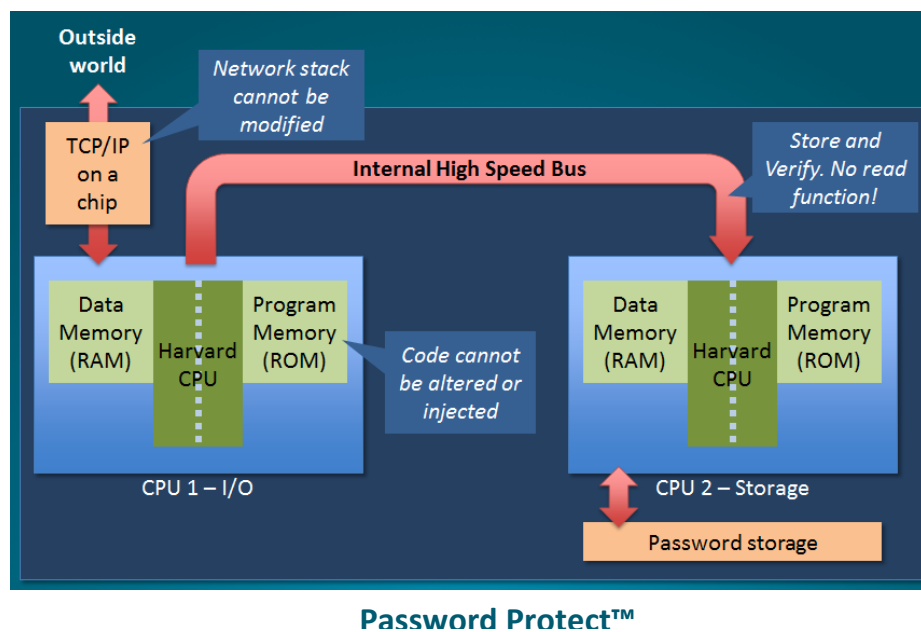With Silicon Safe, these incidents would have been **impossible**

Password Protect

The average internet user has 26 online accounts, and the average cost of a data breach is $164 **per account**. Password Protect is the world's first no-read store for passwords that removes the possibility of bulk theft by attackers.

Conventional approaches attempt to improve security by hardening the operating system, by careful use of privileges, and by encrypting passwords. These slow attackers down, but Password Protect's approach is fundamentally different – it has no operating system, no privileged access, and data is safe whether encrypted or not.

www.siliconsafe.com   **info@siliconsafe.com**

Azure, Facebook, eBay, Google, BIO-key, SafeNet …

Verification

e-Commerce

Verification

Outside world

Network stack cannot be modified

TCP/IP on a chip

Internal High Speed Bus

Store and Verify. No read function!

Data Memory (RAM)

Harvard CPU

Program Memory (ROM)

Code cannot be altered or injected

CPU 1 – I/O

Data Memory (RAM)

Harvard CPU

Program Memory (ROM)

CPU 2 – Storage

Password storage

Password Protect™

Traditional Protection Routes: Harden, Privilege, Encrypt

The Password Database is the Ultimate Target for Hackers. Password databases are protected using three techniques:

1. By **hardening** the applications and the operating system, which consist of millions of lines of code from many authors. Applications and operating systems are breached daily, and exploits like Heartbleed, Shellshock and POODLE show that code written 15 years ago is widely deployed and trusted, yet full of vulnerabilities.
2. Establishing **privilege** levels so that only administrators have read access to secret information. This works as long as the administrator accounts are not compromised. Even worse, if code can be injected into a privileged process space it has full access to everything.
3. **Encryption** of secrets so that, if stolen, they are hard to read. Companies get fined whether the passwords are encrypted or not, and trust is damaged and reputations hurt. Encrypted passwords might be cracked in minutes or years, but the damage has already been done.

Silicon Safe's Password Protect doesn't require these techniques. It uses the minimum required hardware and firmware to perform the task. Password Protect uses less than 5,000 lines of code running on a simple, restricted, hardware platform that completely segregates code and data. **Hardware-enforced, no-read technology is the future of protection for passwords and secrets in the cloud and in the data centre.**

We are defined by what we are: *simple, elegant, unique*; and by what we are not: *no privilege, no keys no OS, no scripts, no SQL, no malware, no leaks, no read, no theft.*

Will Harwood
CTO & Founder

Contact:
Roger Gross, CEO & Founder
+44 787 656 6093

Jon Rolls
+1 571 423 9907

Silicon:SAFE

www.siliconsafe.com   info@siliconsafe.com