What's causing the recent string of data breaches?

October 30 2014, by Jon Tanguy

It's Cyber Security Awareness month, which has me wondering: are we doing all we can to protect our data? To help answer this question, I sat down with Girish Bhat of Wave Systems—an important collaborator of Micron's—to talk all things encryption. Bhat is an encryption guru (AKA, Director of Product Marketing); he shed some light on how data breaches have evolved over the last few years, he waxed poetic about the role of hardware encryption within the bigger "security package," and he stressed the importance of standards and specifications to securing user data. Read our conversation below.

Looking back over the past five years, what's been the biggest change in data breaches? And what's driving this change?

Wave Systems: Data breach disclosures and investigations into potential data breaches are getting a lot of attention from the mainstream media, such as the New York Times, the Wall Street Journal, CNN, CNBC, and the Guardian. Even though data breaches appear to be commonplace today, in most cases, they result from poor security posture—often due to a lack of encryption and a lack of strong authentication.

The recent spate of well publicized data breaches is due to the failure of existing authentication systems to prevent unauthorized accesses and stealing of credentials. With strong two-factor user authentication, most data breaches could have been prevented.

With many enterprise IT departments supporting bring-your-own-device (BYOD) policies, cavalier approaches by employees and partners contribute to the data breach problem. Failure to natively encrypt sensitive data continues to be the Achilles' heel. Relying on user controls and software encryption systems is not serving enterprise IT well. Intentional misuse of sensitive data, as well as inadvertent leaks of sensitive data by insiders, continue to hamper efforts made by IT to mitigate data breaches.

Large enterprises are adopting standards-based self-encrypting drives (SEDs) with remote lifecycle management to minimize data breaches and reduce cost of compliance.

Can you talk about your partnership with Micron, and how Wave Systems' software and Micron SEDs work to secure data?

Wave Systems: Wave Systems and Micron have been working together for several years. Our joint solution provides enterprises with a comprehensive data protection solution at a low total cost of ownership (TCO), and it includes the option of on-premise management or cloud management of high-performance, standards-based OPAL SEDs.

SEDs like those manufactured by Micron are the most secure, best-performing, and fully transparent encryption option for protecting data. Wave Systems provides a scalable remote management platform that helps enterprise IT to deploy, provision, and manage the SEDs in minutes. With Wave's SED management solution, enterprises can easily deploy best-in-class data protection in minutes with full support for advanced capabilities to remotely recover forgotten credentials, remote crypto-erase, and proof of compliance.

With Wave-managed Micron SEDs, IT departments can provide secure audit logs to help workers demonstrate compliance. If a worker loses a device with a Wave-managed SED, there's no guessing or discussions about disclosure. IT can prove that encryption was on by default, so it can prove compliance, eliminating the need for disclosure.

Is there risk of compromising performance when installing hardware encryption?

Wave Systems: There's no risk at all. Software encryption-based solutions are time-consuming and error-prone. It may take up to 10 hours to encrypt a hard drive with software encryption. In contrast, with OPAL SEDs, all data is transparently encrypted using an onboard crypto-processor without any performance penalty. The hardware encryption operation is completely transparent to users—they won't notice it's there. All data is automatically encrypted, and users don't have to identify the data that is sensitive.

Micron has taken a leadership role in the SED market by making solid state drive (SSD) technologies that improve access speeds and provide higher reliability than spinning drives.

Can you talk about the importance of standards organizations for helping to prevent data breaches?

Wave Systems: OPAL SED technology was created and standardized by the Trusted Computing Group (TCG), which is a consortium of experts in the information security industry. The TCG consortium has representatives from leading software, hardware, and drive OEMs and semiconductor vendors, including Wave Systems and Micron. TCG's standards-based approach is extremely beneficial to enterprise IT departments' attempts to mitigate data breaches. IT no longer has to be

locked into proprietary technologies; they now have the capability to swap out a low-performing SED and replace it with a high-performing Micron SED and be compliant in minutes.

Drive encryption is just a small piece of the overall data security puzzle, but it's an important piece. Looking into the future, how do you see the technology evolving to help keep user data safe?

Wave Systems: To keep user data safe, a combination of standards-based, native hardware encryption of data at rest, along with strong control of access to sensitive data using robust, two-factor authentication should be available.

While adoption of an OPAL solution is strong with Windows-based user PCs, laptops, and desktops, continued adoption of mobile endpoints with iOS, Android, Mac OS X, and other systems is critical.

Technologies like OPAL that provide native encryption should be coupled with identity services to provide a device health check when a device starts or resumes to improve overall security posture.

Provided by Micron