Today’s Top Trends in Cyber Security

Protecting information online should be a top priority for all. From encryption and decryption, to block chaining and protecting databases, we rounded up three of today’s most interesting trends in cyber security.

Block Chaining

So what is block chaining? It’s a database of encrypted transactions shared within all nodes in a system. Each transaction within the digital realm contributes to the database with an exact record of the chain of transactions and every block contains a record of the previous block to guarantee the chain’s integrity.

Bitcoin uses this technology to understand who owns what coins. Bitcoin: that purely digital, non-governmental currency you’ve probably read about or maybe even used on the Internet. In previous years it was mostly used illegally but, now that it’s more public, legitimate buyers and sellers are starting to use it. In fact, more than 100,000 merchants around the world now accept Bitcoin as real payment including Dell, Wikipedia, Expedia, PayPal, and many more. But, it’s the underlying bock chain technology used by Bitcoin that is actually the significant idea here.

One of the many benefits of this security technology is that any application requiring a record can now have a system of decentralized consensus because there’s now no one “key” for the system and no single point of failure.

Encryption and Analytics

The more you need to encrypt big data the more it complicates the analysis of that data. This problem seems to have only one solution: Decrypt the data before you analyze it, right?

Wrong. Researchers at MIT found that certain kinds of encryption allow you to perform some kinds of analytics on data, allowing you to only have to decrypt the final results.

A researcher at Stanford, Craig Gentry, found a homomorphic encryption scheme allowing a computer to calculate any function on encrypted data. Although it took quite a lot of effort on the computer’s part, the MIT researchers found a more efficient process using different encryption schemes for different types of calculations.

Many companies are building on this research to find more secure database searches. The big picture idea will be to encrypt and take advantage of stored data without using other computing resources to do it.

Database Protection

A symmetric Database Encryption Key (DEK) is able to encrypt the entire database and is secured by either a certificate or an asymmetric key, depending on the Structured Query Language (SQL) implementation of the database. There are numerous benefits to this idea, but the biggest is that the encryption allows easier compliance with regulations involving data privacy. It also alleviates the need to pre-encrypt data going into the database, simplifies data retrieval, and eliminates any overhead. Also, other applications don't have to be modified to handle this encrypted data, since the data encryption and decryption are managed by the database itself. Finally, you can also choose between Triple DES, AES, and others for the encryption algorithm. Microsoft warns that this encryption is only for data at rest, though.

Keep this protection in mind, considering how much data is being moved to Cloud storage now.

For any general encryption rules, follow Microsoft's directions:

- Strong encryption tends to use more CPU than a weak encryption
- Long keys tends to yield stronger encryption than short keys
- Asymmetric encryption is weaker than symmetric encryption using the same key length
- Block ciphers with long keys are stronger than stream ciphers
- Long, complex passwords are stronger than short passwords
- Are you encrypting lots of data? You should encrypt using a symmetric key and then encrypt the symmetric key with an asymmetric key
- Encrypted data can't be compressed, although compressed data can be encrypted

Research summarized from a November 2014 article in Computerworld: www.computerworld.com/article/2851414, an October 2015 article in Security Info Watch: http://www.securityinfowatch.com/article/12116284/tech-developments-in-cyber-security, an article from IEEE Spectrum magazine: http://spectrum.ieee.org/computing/software/how-to-compute-with-data-you-cant-see, and from Microsoft SQL encryption information: https://msdn.microsoft.com/en-us/library/ms189586.aspx.