A Simple Solution to Prying Eyes

BY DON RIMA

Life used to be simple. People didn't have credit cards or rely on Social Security numbers as identifiers. We didn't have people losing laptops containing sensitive data—and if we did, who'd want it? Identity theft wasn't a phrase that was as common as corn flakes. Ah, the simplicity!

Life's changed. Now, we must secure not only the doors to the server room, but also the very field elements and their contents. People started losing data or availing themselves of data the rest of the world didn't want them to have. Then networks were born and before long people could sniff other computers. Networks led to the Internet and, from there, it was an information free-for-all.

Industry then turned to, among other things, cryptography to protect what was becoming its largest asset—data. People just didn't want anyone creeping in over their networks and sniffing into datasets that they weren't supposed to be sniffing in.

The IBM* System i* platform is no exception to these concerns. Even though the underlying operating system provides a strong, integrated security model, the need still exists to secure data down to the field element. That's where cryptography comes in handy. This month I look at Crypto Complete from Linoma Software (www.linomasoftware.com).

Installation

Installing the product from CD isn't hard at all. But that's only the first step. You then need to set up your key officers and keys. The Linoma folks can give you some advice on ways to consider doing this, based on your installation and needs. It's not complex, but spending a little time thinking out how you want it done can save you some problems down the road.

Also, security and encryption standards, from a corporate level, vary from company to company. I suggest reviewing your company's internal procedures and policies with your auditors to make sure that your setups will be in internal compliance.

Spotlight Profile

Product: *Crypto Complete*
Company: *Linoma Software*
Version: *1.2*
URL: *www.linomasoftware.com*
Overall Rating: *3.715*

Ease of Use

You'll have some decisions to make once you start using the product, like how and where the field encryption takes place. Depending on what kind of field you're encrypting, part of that decision will be made for you. For instance, if you're encrypting a numeric field, the result will be an alpha field and most likely longer than the original numeric. Crypto Complete makes provisions for either storing the encrypted values within the current file or in an external repository. Then you need to decide how the ongoing maintenance is done; your programs can call the APIs or Linoma can place triggers on the file to automatically encrypt values as they're added or updated.

Linoma provides some nice sample RPG source code that you can cut and paste into your applications. The rest of the application is a series of menus that walks you through the commands around the product.

I found myself wishing for additional prompting in areas. For example, when adding a field name, I couldn't remember the name of a field or its type attributes and had to exit the process, get them

The Rima Report

Category	Points	Weighting	Overall Score
Certifiability	4.000	.100	0.400
Installation	3.700	.150	0.555
Ease of Use	3.600	.150	0.540
Documentation	3.500	.150	0.525
Functionality	3.800	.150	0.570
Usefulness	3.800	.150	0.570
Support	3.700	.150	0.555
Total	26.100		3.715

KICK THE TIRES: If you have field-level encryption needs and don't want to roll your own, you should consider this.

(Points given are on a scale of 0 to 4, with 4 being the highest. Each category is assigned its own weighting from the total of 100 percent.)

from the Display File Field Description (DSPFFD) command, write them down and restart.

Documentation

Both the user's guide and the programmer's guide are well done.

Certifiability

Everything I tried worked as I expected.

Functionality/Usefulness

This product meets a specific protection need nicely. Once you finish the initial setup and get the hang of it, field-level protection is really no big deal and you won't likely think much about it.

Keep in mind that this is basically for stationary-table field encryption. It's not for data-transmission encryption or file encryption. Further, it only uses symmetric encryption algorithms, which in my opinion are fine for a table- or field-level basis. If you want something like Pretty Good Privacy with long key lengths, well, it's not this product.

One of the big issues with encryption is key management. This product allows for multiple versions of a key to be used concurrently. For example, if a field is encrypted with the key used on day one, then keys are changed on day 90, the product knows which key to use to decrypt. All encrypted field adds or updates should use the latest key. After a while, you'll have a lot of keys around. Periodically, you may want to consolidate your keys and data into the current key. There's no good way to do that currently (you have to deactivate then reactivate the field) but it's on the list of items for the next release. The new features should let you to sweep a field's encryption history and reset it using the current key settings.

Support

What the tech support folks didn't know immediately, they were able to find quickly. Everything went smoothly.

What I'd Like to See in the Next Release

- Prompting for field names
- Simpler key consolidation (planned for a future release)

Summary

I think Linoma has another nice niche-product hit on their hands. With Crypto Complete you can provide good field-level protection for your existing and developing applications with minimal impact on your programming staff. It could be a simple answer to the complex problem of prying eyes.

The coding examples are easy to follow and incorporating this product into your IT shop should be pretty effortless. Your only concern will be to make sure you're within your company's data-protection policies when doing the setup, but my guess is that in many cases you'll be writing these policies as you go. Welcome to the world of the midrange shop.

Don Rima *has more than 20 years of experience with IBM midrange systems. He can be reached at dr2@dlr2.net.*