Defending Encryption

Will Holcomb

CSC 203 - September 16, 2002

> James Bidzos, president of RSA Data Security, offered an analogy to the concern about criminal use of secure encryption. He suggested that law-enforcement agencies could have made similar arguments against the building of the interstate highway system. Criminals could flee to different states or transport stolen goods across state lines. We recognize that, yes, these are indeed problems, but economic and personal benefits from a safe, convenient, efficient transportation system outweigh the problems.

I think that Bidzos' fundamental analogy is a good one in that encryption does enable certain methods of "transport" that would not have been feasible otherwise. The interstate system deals with connectivity and throughput whereas encryption deals with security, but in both situations they make available a method of transport. Much the same as it is not realistic to expect semi-trucks to make regular cross country trips on back roads, it is not realistic to expect explorable traffic like bank account information to make it across the open Internet securely without being encrypted. [Interestingly one of the major reasons for developing the interstate system was security; specifically to allow troop movements around the country should war ever make it to American soil.]

I don't especially like how the argument is framed however. Business is in many ways sacrosanct in our country in ways that personal liberties are not. The right to earn an income ranks fairly high among the protected liberties. I personally think that personal use of encryption is as much about an individual's right to privacy as it is about protecting business interests. I can understand how Bidzos, likely speaking to a corporate audience, would choose this aspect of the benefits of encryption.

Honestly, monitoring the Internet is something that is going to be almost impossible on any reasonable scale unless it changes in some fundamental ways. Say encryption were outlawed and people who are using it for illicit purposes were somehow forced to stop sending encrypted data directly. The field of stenography is fairly well developed and checking all of the traffic on the Internet for stenographic encodings is next to impossible and even if you find one, you can encrypt the contents of the message. The long and the short of ti is, if people want to find a way and are sufficiently determined, they will find a way. All that can be done is to make the process more inconvenient.

There are other uses for encryption that securing network traffic of course. Encrypting personal file for various reasons. I am running tripwire on my Linux box and that file in encrypted, so even if someone breaches the system they can delete the file, but they can't falsify it. Certainly this sort of encryption is useful for keeping criminal information hidden. Physical security is useful in the same way. The Internet, in particular, is an untrustworthy place. In such an environment the ability to keep secrets in crucial and the value of encryption cannot be underestimated.

Honestly, the way that things are right now is probably the best. We have encryption that the CIA can probably break trivially. It gives people a sense of security that prevents people from working to hard to find new methods of encryption, and also protects casual eavesdroppers from finding out secrets.