GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Key Escrow Encryption: Would It Have Saved the Day?

Jon Moses

Version 1.2f

Shortly after the events of September 11th, 2001 there were a great many bills introduced into congress. Some of these bills dealt with encryption, and how to prevent criminals from using it to conceal their crimes, or plans about future criminal activity. Some of these bills put forth the idea that all encryption must be key escrow encryption. Key escrow encryption means that when you encrypt something with your secret key, another secret key must be stored somewhere, in "escrow," so that your data can be decrypted if you lose or forget your key. This paper will try to explain, in layman's terms, what key escrow means in detail, and why key escrow policies would not necessarily have stopped the events of September 11th.

Cryptography is "the art and science of keeping messages secure" (Schneier, 1). What that means is this: pretend Alice wants to send a letter to Bob, and she wants to make sure that Bob, and only Bob, can read it. She would use cryptography to do this. More specifically, she would use encryption, which is "the process of disguising a message in such a way as to hide its substance" (Schneier, 1). When you encrypt a message, or plaintext, you get ciphertext, which is the encrypted message. The opposite of encryption is decryption, which turns ciphertext into the original plaintext.

When Alice encrypts the letter to Bob, she uses a cryptographic algorithm, or cipher, which is a "mathematical function used for encryption and decryption" (Schneier, 2). She takes the ciphertext and sends it to Bob, who then decrypts it into plaintext and reads it. Now, when Alice encrypts the letter, she needs to give the cipher some extra information. This information is called a "secret key" and it provides the security. If the cipher did not need a key, anyone that gets the ciphertext could decrypt the message with the correct cipher. With the use of a secret key, only someone with the secret key can decrypt the message. This ensures that only the people that are supposed to read the letter can. The whole encryption/decryption process can be abbreviated like so: $E_k(P) = C$, for encryption and $D_k(C) = P$, for decryption. What this means is when you encrypt (E) the plaintext (P) with a secret key ($_k$), you get ciphertext (C); and when you decrypt (D) the ciphertext (C) with the same secret key ($_k$), you get the plaintext (P) you started with. This notation will be used throughout this paper.

There are many legal uses for cryptography. The most common use is to prevent other parties from reading confidential documents. This is used by governments, businesses and many "normal" people. It is easy to see why governments and businesses would want to prevent other people from reading their information, but why would anyone else? Simple, pretend that Alice is going on vacation, and she wants Bob to feed her fish. For some reason, Alice won't see Bob before she leaves, but she needs to tell him where the key is. If she just sent a letter, or an email, telling him where it was, a robber, Charlie, might read that letter, and be able to get into Alice's house with no trouble at all. If Alice uses encryption, she can be sure that only Bob can read the letter, and that only he will know where the key is. This is just one example of the many reasons that "normal" people would use encryption.

Key escrow encryption is very similar. The only functional difference is that there

© SANS Institute 2000 - 2005 Author retains full rights.

are two secret keys, and decryption can be done with either one. One of the keys is used by the two parties, the other is stored, or escrowed, in some secure location, to be used if the original key is forgotten, or more likely, by law enforcement if they suspect the two parties are engaged in criminal activity. It is important to note that when key escrow encryption is used and law enforcement wants to use the escrowed key, they do have to obtain a warrant. This is the kind of encryption that many people believe should be all that is available to the general public.

For a little more detail, let's look at key escrow encryption expressed in the notation discussed above. Encryption would look like this: $E_k(P) = C, {}_k{}^2$. This means that when the plaintext is encrypted with a secret key, you get the cipher text, which is just like normal, but you also get a second key (${}_k{}^2$), which gets escrowed. Decryption would look like this: $D_k(C) = P$ and $D_k{}^2(C) = P$. The first part looks exactly the same; when you decrypt the ciphertext with the secret key, you get the plaintext. This second part is what's different, and what the government is interested in. When you decrypt the ciphertext with the second, escrowed, key (${}_k{}^2$) you also get the plaintext. This is the idea that key escrow systems revolve around; the ability to decrypt the ciphertext with the second key, the one that gets placed in a central repository.

There are some pluses to key escrow. One of the biggest pluses is that it allows law enforcement to access encrypted messages of suspected criminals. This, in my opinion, is also the biggest minus, but more on that later. The escrowed key can also be used if the original secret key is forgotten, which is likely to happen. This prevents the encrypted data from being lost permanently.

Another plus is that if you lose or forget the original secret key, you can still recover the data using the key that was escrowed. To see how that would be helpful, take this example: you're the CFO of a large company, and all the company's financial records are stored encrypted; the person in charge of encrypting and decrypting leaves, and takes the secret key with him. If the records are encrypted in a normal, one secret key, scheme, there is almost no hope of ever recovering those records, but with a key escrow system there is every hope of recovering them. The escrowed secret key will also decrypt the records, which can then be re-encrypted with a new secret key. The same thing can happen if you forget a secret key, you can recover the data with the escrowed key.

There are also minuses to key escrow. The biggest is that any cipher that implements key escrow encryption is inherently weaker than those that don't. A recent report on the state of key escrow systems states that "Most of the key recovery or key escrow proposals made to date, including those designed by the National Security Agency, have had weaknesses discovered after their initial implementation" (Abelson, 3.2). What this quote means is that, to date, any key escrow system that has been proposed, and then implemented, has had weaknesses that would allow unauthorized people to get the plaintext of something from the ciphertext.

This is the case because key escrow systems are much more complex to design, and test. With a non-key escrow system, there is only one way of decrypting the ciphertext. Because of this fact, there is really only one way to decrypt the data if you don't have the key. It's called a brute-force attack, and it involves checking every possible key to see if it decrypts the data. This is a reliable method, but it takes a very

© SANS Institute 2000 - 2005 Author retains full rights.

long time. For example, there is one popular encryption algorithm, DES, that takes variable length keys. Key lengths are measured in "bits," which are just binary digits, ones and zeroes. There was a machine built in the late 1990's which could crack a 56-bit DES key in under a day. This makes for a very poor level of security, but by simply increasing the key length from 56 bits to 128 bits, you get an extremely high level of security. If the time it took that machine to crack the 56-bit key were reduced to one second, it would take 149 trillion years to crack the 128-bit key (PCDynamics).

With a key escrow scheme, there are many more places where the system can be compromised. The first is the same as a normal encryption scheme; the key can either be stolen or brute-forced. The other vulnerabilities come when you add the support for additional keys. The key escrow component that is responsible for creating and managing the other keys could be subverted to either send the keys to the wrong place for escrow, or to create more keys that the user wants, thus allowing more people to access the data. Another additional component, which controls the decryption by the other keys, might have weaknesses that are not present in the encryption scheme. This would allow people to access the data without having any of the keys, but rather by exploiting problems with the data recovery side. (Denning)

These are just some of the technical problems with key escrow encryption schemes. Next I'll be discussing some of the other problems that I see with key escrow. These problems focus more on the practical application of key escrow, and with the probably misuse of such a system.

The first problem, which in my opinion is the biggest, is that of where to store the keys. If a key escrow system is mandated, the big question is what is done with the keys? Sure, it's great that the government would want to get backdoor keys to our encrypted data, but where would they put them? My fear is that they would put them in some huge database in some government installation, on a government network, linked to the Internet. This would not be a smart idea, because if the machine is attached to the Internet, no matter how many security measures are taken, the machine will be compromised once people know what's on it.

My fear here is that the government will not understand what these keys would represent. These keys wouldn't just be keys to encryption; they are, in essence, the data that is encrypted. That data would be everything from emails to confidential medical records to proprietary business secrets. If the keys are not treated as such, it greatly increases the chance that they will fall into the wrong hands. For example, if the keys were stored on a computer that was accessible from the outside world, and someone successfully attacked that computer and gained access to the keys, they could then access all the data that had been encrypted. This would set the stage for either espionage or blackmail, or even both.

In order for a central repository for encryption keys to be feasible, it must be accorded the same importance as other national secrets. I feel that the keys must be guarded with the same security as our nuclear launch codes. The codes are kept so secret that we, the public, don't even know where in the country they are stored, much less how. If the escrowed keys were given that much security, then perhaps my fears about the keys getting stolen would be laid to rest.

Another concern is the misuse of the keys by the government. For example, if the

© SANS Institute 2000 - 2005 Author retains full rights.

government thought that someone was planning to commit a crime but the only communicating that person did was encrypted, the government might use an escrowed key to find out what the contents of the communications were. In certain situations, this is fine; in fact, it's the whole point of the key escrow system. I feel that the use of the keys in this situation should be similar to, but more restrictive than, wiretaps. A wiretap must be applied for, to a judge, with certain information on the application: who requests the wiretap, who it's against, why it's needed, etc (USC). This is so that an average law abiding citizen is relatively safe from having their conversations overheard and recorded. I would support key escrow if a similar system were put into place for the use of keys that have been escrowed. I do feel that it should be more restrictive, as the keys not only would give access to communications, but also to any electronic data that had been encrypted such as: financial records, personal data, medical records, etc. This additional access merits additional restrictions.

While it is important to discuss the benefits and negatives of using a key escrow system, there is a more important question: would it have prevented the events of 9/11? The short answer is no. While a key escrow system might stop petty criminals who don't really understand that the crypto they are using has a backdoor in it, major criminals will understand that, and they will not use that kind of system. The United States is not the only nation in the world that develops crypto systems, and the criminals would just obtains encryption that did not have a key escrow scheme embedded into it. Yes, it would be against the law, but criminals, by definition, don't really care. The use of a non-key escrow encryption scheme may mean the difference between a 2-year sentence, for using illegal encryption, and a lifetime sentence, for planning a terrorist attack.

It has been speculated that the suspected mastermind behind the attacks of 9/11 is Osama bin Laden. The government says that bin Laden and his network are using "uncrackable encryption…to communicate about their criminal intentions" (USA). The government uses this, along with other examples, as arguments in their fight for a mandatory key escrow system.

The question is whether a key escrow system would have prevented, or warned us about the terrorist attacks on 9/11. First, we'll pretend that there is no other encryption but the key escrow kind available, which isn't true. Next we'll look at what bin Laden has done to prevent people from knowing what he is doing, and apply that kind of strategy to the use of key escrow encryption.

Right now, the government is trying to learn where bin Laden is, and what he's going to do next. They are doing this in a variety of ways. I assume that they are monitoring all the cellular calls in Afghanistan, if there are any cell towers, and that they are most assuredly monitoring the radio waves. I'm sure that they are doing other things, but those suffice for now. Apparently we used to know where bin Laden was and who was in his organization, just by tracking his use of a satellite phone and by monitoring his email. Now, we have no idea where he is. How is that possible? The answer is very simple. He stopped using his phone and stopped sending email. Now we have no idea where he is.

Yes, it's that simple. Osama bin Laden knew that we were monitoring his fancy high tech gadgets, so he simply stopped using them. "This isn't low-tech," a former NSA consultant has been quoted as saying. "You'd have to really call it no-tech" (Register).

© SANS Institute 2000 - 2005 Author retains full rights.

Now, let's take that strategy and apply it to the whole key escrow encryption idea. Here it is, bin Laden's been using encryption that the government can't break, and for some reason, the only encryption that he can get is key escrow encryption that will allow any government to read his email. What does he do? Yes, he stops using encryption altogether and starts sending people as messengers. That's it. Simply by not using encryption and by sending messengers, he avoids the key escrow trap. The U.S. is now foolish looking, but they can read your email, if they really want to.

What does all this really mean? Well, it means this: key escrow systems won't stop terrorists like the government says. It might do other things, like help the government catch dumb criminals, which then would "prove" that the system works, but that's it. One more thing that it would do is open up a whole new avenue for espionage and black mail. Once all those keys are in one place, it's only a matter of time before someone manages to break into where they are and steal them. Whether they are stored digitally, in a computer system, or on real paper, someone will get them. And even if no one steals the keys, the encryption schemes that use key escrow are harder to test, and therefore will most likely contain holes that no one will know about until that hole is exploited and all the encrypted data is unsafe.

There are more sides to the issues of mandatory key escrow systems than have been discussed here. For example, I didn't even touch the civil rights or privacy issues, and I don't feel that I need to. With all the negatives to the whole issue, I feel that mandatory key escrow systems will never work, even if a law is passed about them. Other governments apparently feel the same way. In May of 1999, British parliament refused to sign into law a bill that would make key escrow encryption mandatory. "The committee said it saw no benefit in the most contentious part of the Bill - key escrow and key recovery" (TechWeb). Hopefully other governments will take heed of what the British have done, and act accordingly.

To sum up, I don't believe that any kind of key escrow encryption would have stopped the events of 9/11 because there are just too many ways to communicate securely without even resorting to encryption. The only thing that encryption did for bin Laden was make it easier to do. Key escrow encryption would only make it harder to communicate securely, not impossible. The emphasis needs to be on things that will help, like better human intelligence from our intelligence agencies, not things that will make the government and the public feel better, like key escrow encryption.

© SANS Institute 2000 - 2005 Author retains full rights.

Bibliography

Abelson, Hal, et al. The Risks Of "Key Recovery," "Key Escrow," and "Trusted Third-Party" Encryption | 1998. http://www.cdt.org/crypto/risks98/ (10 Nov. 2001).

Denning, Dorothy E. A Taxonomy for Key Escrow Encryption Systems. http://www.cs.georgetown.edu/~denning/crypto/Taxonomy.html (10 Nov. 2001).

PCDynamics. SafeHouse FAQ. http://www.pcdynamics.com/SafeHouse/SafeHouseFAQ.asp (10 Nov. 2001).

The Register. "Feds complain bin Laden not using high-tech equipment." http://www.theregister.co.uk/content/57/21790.html (10 Nov. 2001).

Schneier, Bruce. Applied Cryptography. New York: John Wiley & Sons, 1996

TechWeb. "Key Escrow Bill Slammed By Parliament Inquiry." http://content.techweb.com/wire/story/TWB19990519S0001 (10 Nov. 2001).

USA Today. "Terror Groups Hide Behind Web Encryption." http://www4.law.cornell.edu/uscode/18/2516.html (10 Nov. 2001).

United States Code. Title 18, Section 2516: "CHAPTER 119 - WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS." http://www4.law.cornell.edu/uscode/18/2516.html (10 Nov. 2001).

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.