

On the other hand a large frame in a fast moving sequence, say a sporting event, could generate a lot of data even after compression and take so long to encrypt that the delay causes a deterioration in quality. Therefore a good video encryption algorithm should limit itself to a maximum number of encrypted bits per frame, regardless of the frame size. Tests have shown that it is possible to do this while still creating un-viewable encrypted streams. This has been demonstrated for example for RVEA (Realtime Video Encryption Algorithm) developed at Purdue University in the US.

The question arises of whether such algorithms operating on a relatively small number of bits in the video stream are sufficiently immune from attack, given that huge computational power is readily available to many hackers these days. If only a limited number of bits are encrypted, it might seem that the chance of decrypting the video through brute force trial and error is increased. But the task is greater than it appears for two reasons. Firstly if the encryption is operating on compressed MPEG transport streams, as is the case with RVEA for example, the cost of any attack would be increased because the MPEG decoding process also has to be performed.

Secondly an attack involving trial and error testing would depend on the computer being able to tell when a video frame that is comprehensible has been produced. Although computers can distinguish individual items such as faces when presented with clearly defined images of the same form, they cannot at present identify whether a video frame is a meaningful image for a human rather than just a random assortment of bits. This after all is a somewhat subjective distinction depending on the context, and cannot be readily defined. It might be possible in some cases to obtain blurred pictures via trial and error by having a human watching a quick replay of candidate images produced by a powerful computer, but it would be a long and tedious process to recover the full video stream this way.

Not all video is encoded via MPEG of course, and video conference software normally uses the H.263 protocol. Encryption of such data will also become more important as the Internet grows as a medium for on-demand video conferencing. In some respects the encryption requirements will be more conventional, being to avoid eavesdropping and maintain privacy during sessions. The focus is on the network and the systems that control the sessions

rather than the end point devices and interfaces. The main concern would be to avoid people listening in to what could be confidential sessions involving sensitive or valuable information within the content rather than theft of the video content itself. In this case there might be an argument for a stronger level of encryption than for broadcast video within the network, although in practice Internet video conferencing is unlikely to be used for high-level interaction.

But another difference is that Internet conferencing is relatively low quality at present, running at the same data rates as other applications. Therefore it can be served by the same encryption mechanisms, which could be SSL in conjunction with a private key system such as DES. At present however many Web based conferencing services do not support within their client software, which should deter business users.

The real interest though concerns digital video broadcasting both to PCs and TVs, given the desire on the part of content owners to lock up as many sources as possible. For consumers this will mean that the great broadcasting revolution may not be as liberating as had been hoped, given an unholy alliance of regulation, litigation, and access control.

The question of organizational forensic policy

Hank Wolfe

The objectives of an organization in combination with the formal policy together underpin the strategic direction that any organization will take. We all know that security begins with policy – in other words the rules of play. If policy is sound then the appropriate security measures can be implemented to protect the activities required to achieve the stated objectives as well as maintain the information assurance requirements – availability, integrity, authentication, confidentiality and non-repudiation.

Policy fails when management does not actively support and promote it. The two top executives of a very large local organization have continually refused to accept and adopt the formal policy document proposed

by the professionals responsible for creating it. The reason is that the two individuals have not changed their password in eight years and see no reason to be forced to do so regularly – a best practice as proposed in the

new formal policy. Management is either part of the problem or part of the solution. These two should most probably be engaged in a different line of work because they compromise their organization's security and set a bad example for their subordinates.

New policy is now needed to cause the appropriate procedures to be put into place such that if and when an incident occurs (criminal or one that requires internal discipline) there is a mechanism in place to protect any potential evidence that may be needed to deal with the offender(s). This is no longer a trivial issue and will become even more important in the future. It too will require the active support of top management. This article is about creating a security policy that deals with forensic evidence.

What is forensic evidence?

In computing, forensically we are able to collect many different facts from computer media that can now be used in a court of law. Much of the data that may qualify as evidence resides on hard drives in obscure places that most users are not aware of. The forensic investigator must first capture an evidentiary copy of the data residing on computer media associated with the case, and that includes hard drives, floppy disks, CDs, DVDs, flash cards, PCMCIA cards, etc. This evidentiary copy must be validated by using hashing algorithms to prove that the original data and the evidentiary copy of it are exactly the same. The success or failure of a prosecution or disciplinary action may rest first on the validity of the capture process and then on maintaining the chain of evidence. Thereafter, the investigator will be engaged in the analysis and reporting of any evidence that is ultimately found and occasionally testifying in a court of law as to the specifics of how that evidence was obtained.

Forensic policy

For purposes this discussion, every organization of any size should be considering the creation of a policy and formalized set of procedures that describe and document the actions that will be taken when an incident is discovered.

Many will assume that all that is necessary is to assign the task of capturing evidence to the most technical person available within the organization. If that person is trained in forensic evidence gathering AND if that person has the appropriate tools to accomplish the task then the likelihood of success is enhanced. Merely assigning the task to the most technically competent assures nothing and will most likely not be successful. Technical competence is not enough.

When I first began my career in the computing profession, there were only a handful of people in the entire world that knew how to write a program and operate a computer. Today there are literally tens of millions of people who can do that. It seems that just about everyone who has

pushed a mouse around for six months or a year has become a “computer expert”. Be assured that they are not and that there is much happening underneath the operation of a mouse and the applications that can be launched by it. While these “experts” may know how to get the most from any given software application, it is unlikely that they have any idea of what happens when the computer is turned on – the boot process, the loading of the interrupt table, how that interfaces with the BIOS, etc. Most users and many so called experts do not know what happens in the registry or what the swap file is used for or how data is actually physically stored on any given media. Many do not even know that a file that has been deleted is not removed from the device and remains there unchanged until its space is overwritten (hard drive, floppy, etc.).

*Electronic forensics
draws on computer
science, police
science, cryptography,
surveillance and
common sense.*

Forensic investigators must have this basic knowledge and much more to effectively capture and investigate any given case. In fact, merely turning a machine on makes changes to the hard drive of that machine and in so doing may negate the potential evidence that may be found there. Electronic forensics draws on computer science, police science, cryptography, surveillance and common sense.

Because of these facts, the procedures to be followed when an incident is discovered need to be closely controlled and formally documented. What is being proposed in this discussion is that this activity be recognized in a series of formal policies and formulated in a set of documented procedures. Most organizations do not need a forensics investigator on staff and that is not what is being recommended. However, there should be someone who has been

minimally trained in the basics of forensics and is responsible for handling any given incident once it has been discovered. This may be as simple as locking down the suspect machines and ensuring that they are not used or tampered with until a trained forensic investigator takes control of the case.

Conclusion

Every organization of reasonable size should address this issue. It doesn't require huge outlays of capital or a large investment in equipment or software (unless the organization plans to set up its own forensic laboratory). Creating a policy after some investigation, in the scheme of things, is very inexpensive and may mean the difference between a successful and unsuccessful prosecution. Retaining a forensic investigator is also an option and their services could be called upon when an incident is discovered. Finally, it must be understood that a proper forensics investigation takes time. It cannot be done in a few minutes or a few hours. Time is money and it must be clear that such investigations cost money AND there is no guarantee that relevant evidence will be found.

About the author

Henry B. Wolfe has a long computing career spanning more than 45 years. He currently specializes in cryptographic problems where related to forensic investigation, general computer security, surveillance, and electronic forensics teaching these topics to law enforcement (both in New Zealand and internationally) as well as at the graduate level in the University of Otago located in Dunedin, New Zealand where he is an associate professor.

Contact:

Dr. Henry B. Wolfe
University of Otago
New Zealand
Phone: (+64 3) 479-8141
Email: hwolfe@infoscience.otago.ac.nz