WIKIPEDIA

Traitor tracing

Traitor tracing schemes help trace the source of leaks when secret or proprietary data is sold to many customers. In a traitor tracing scheme, each customer is given a different personal decryption key. (Traitor tracing schemes are often combined with conditional access systems so that, once the traitor tracing algorithm identifies a personal decryption key associated with the leak, the content distributor can revoke that personal decryption key, allowing honest customers to continue to watch pay television while the traitor and all the unauthorized users using the traitor's personal decryption key are cut off.)

Traitor tracing schemes are used in pay television to discourage pirate decryption – to discourage legitimate subscribers from giving away decryption keys.[1][2][3][4][5] Traitor tracing schemes are ineffective if the traitor rebroadcasts the entire (decrypted) original content. There are other kinds of schemes that discourages pirate rebroadcast – i.e., discourages legitimate subscribers from giving away decrypted original content. These other schemes use tamper-resistant digital watermarking to generate different versions of the original content. Traitor tracing key assignment schemes can be translated into such digital watermarking schemes.[6][7][8]

Traitor tracing is a copyright infringement detection system which works by tracing the source of leaked files rather than by direct copy protection. The method is that the distributor adds a unique salt to each copy given out. When a copy of it is leaked to the public, the distributor can check the value on it and trace it back to the "leak".

Primary methods

Activation controls

The main concept is that each licensee (the user) is given a unique key which unlocks the software or allows the media to be decrypted.

If the key is made public, the content owner then knows exactly who did it from their database of assigned codes.

A major attack on this strategy is the key generator (keygen). By reverse engineering the software, the code used to recognise a valid key can be characterised and then a program to spit out valid keys on command can be made.

The practice of traitor tracing is most often implemented with computer software, and evolved from the previous method of activation codes. In this model, each box of software ships with a unique activation number on a sticker or label that can only be read after the package is opened, separate from the CD-ROM or a DVD-ROM. This number is an encoded serial number, expanded to a usually large number or string of letters, digits, and hyphens. When the software is being installed, or the first time it is run, the user is prompted to type in the license code. This code is then decoded back to its base serial number. This process reduces the number in complexity, and the additional information removed by this process is used to verify the authenticity of the serial number. If the user mistypes a single character in what is sometimes a very long code, the software will refuse to install and require the number to be retyped until it is correct.

This activation code is generated during the packaging phase of manufacture, so that every user is

receiving the same software but a different activation code. If a user performs a "casual copy" of the software for a friend, that friend must have the license code as well as the software to install it on their system. Since the software itself cannot determine that it is a copy, this is a way to beat this basic system.

With the expansion of computer networking, two additional levels of software protection have evolved, "network registration" and "online registration".

Network registration

Software that employs this additional security keeps a copy of the actual serial number being used in the license code. When it is active, it is broadcasting this number on a clandestine channel on the local network. If the software has been installed on another computer on that same network, using the same license code, when the second copy is run it will detect its serial number in use on the network and typically will refuse to run. It may also cause the other copy of itself already in use to close. This prevents a small business from buying one copy of expensive software and installing it on several of the computers at their location, provided they are networked.

Online registration

The process of online registration is very similar to activation codes, but adds an additional step. Most modern companies are now not only internally networked, but are also connected to the internet. This allows the software manufacturers to add an additional check to their system during the installation process. When the user enters a valid license code, the software does not immediately install. Instead, it uses the active internet connection to contact a server being operated by the software manufacturer. The license code is transmitted to the server, and it waits for the server to tell it whether the install should be permitted. The server maintains a database of all the serial numbers that have been used to install their software. If a single serial number is used on a number of machines (a typical limit would be five machines) then the server tells the software that it is likely a copy and to abort the installation. The users are usually presented with a dialog instructing them to contact the manufacturer.

Watermarking

Websites offering subscriber downloads may embed a digital watermark in the download, usually in a way that is not readily apparent to the user. For example, an identification number may be embedded in an image, or in metadata such as the date of a file. It is also possible to watermark multiple copies of a file with a unique watermark per recipient before sending them. In this case the embedded identification number can be the ID of the recipient.

Other methods

Some software that implements online registration extends this with a process commonly known as "phoning home". In this case, the software, either each time it is used or at some preset interval such as monthly, makes another connection back to the registration server. It does this to check in with the server to see if the serial number it is using has been determined to be one that is being used to install in many places. Serial numbers that have been identified as "pirated" (illegally distributed) are added to a blacklist on the server, a process referred to as being "burned". Burned serial numbers cannot be used to install or activate the product. Serial number lists are available on the internet that include a large number of valid registration codes for many software titles. It is common for software manufacturers to seek out these lists and invalidate the serial numbers that appear on these lists. This discourages individuals from giving out their registration codes for fear that this code will later be invalidated, disabling the original install of the

software the next time that it "phones home".

Some of the more expensive software requires the user to send personal information to the software vendor before receiving the activation code. The activation code is usually a large sequence of numbers and letters, and encodes information including the license serial number, information to ensure the code is valid, and also includes the ability to verify the personal information the user sent to the software vendor. In this way, the user's name or business name must be entered along with the registration code. The registration code will not be accepted by the software unless the user types in the business name exactly as submitted to the software vendor. The business name is usually displayed by the software on its opening banner whenever the software is used. If the customer gives away his activation code it will be useless without his business name, and anyone that uses the activation code must enter it in during the activation process, leaving the original buyer's business name on the banner of the software. This makes it very easy to "trace the traitor" and find any customers who originally gave out their activation codes. Since giving away the registration code is a violation of the license agreement, the software vendor may invalidate the user's serial number (disabling that user's software in the process) and may take legal action. This does raise privacy concerns in some areas.

See also

- Canary trap

References

1. Benny Chor, Amos Fiat, Moni Naor, Benny Pinkas. "Tracing Traitors" (http://web.cs.ucla.edu/~miodrag/cs259-security/chor94tracing.pdf). 1994.
2. Benny Pinkas. "Traitor Tracing". doi:10.1007/978-1-4419-5906-5_158 (https://doi.org/10.1007%2F978-1-4419-5906-5_158). 2011.
3. Ryo Nishimaki; Daniel Wichs; Mark Zhandry. "Anonymous Traitor Tracing: How to Embed Arbitrary Information in a Key" (https://www.cs.princeton.edu/~mzhandry/docs/papers/AnonTT.pdf) Archived (https://web.archive.org/web/20161012225051/https://www.cs.princeton.edu/~mzhandry/docs/papers/AnonTT.pdf) 2016-10-12 at the Wayback Machine. p. 1.
4. Dan Boneh; Mark Zhandry. "Multiparty Key Exchange, Efficient Traitor Tracing, and More from Indistinguishability Obfuscation" (https://eprint.iacr.org/2013/642.pdf). 2013. p. 5.
5. Michel Abdalla; Alexander W. Dent; John Malone-Lee; Gregory Neven; Duong Hieu Phan; and Nigel P. Smart. "Identity-Based Traitor Tracing" (https://www.di.ens.fr/~mabdalla/papers/ADMNPS07-a4.pdf). 2007.
6. Amos Fiat; Tamir Tassa. "Dynamic Traitor Tracing" (http://www.cs.tau.ac.il/~fiat/dyntt.pdf). doi:10.1007/s00145-001-0006-7 (https://doi.org/10.1007%2Fs00145-001-0006-7). Journal of Cryptology. 2001. pp. 212–213.
7. Tamir Tassa. "Low Bandwidth Dynamic Traitor Tracing Schemes" (https://www.openu.ac.il/lists/mediaserver_documents/personalsites/tamirtassa/lbdtt.pdf). Journal of Cryptology. 2005. pp. 167-183.
8. Xingwen Zhao, Fangguo Zhang. "Traitor Tracing against Public Collaboration" (https://eprint.iacr.org/2011/084.pdf). 2011. p. 2.