

IRDETO ACTIVECLOAK™ CORE TECHNOLOGY: THE KEY TO EFFECTIVE CONTENT PROTECTION

THE MEDIA APPLICATIONS DRIVING THE TV EVERYWHERE REVOLUTION RUN ON INCREASINGLY OPEN PLATFORMS AND REQUIRE A MORE ROBUST AND HOLISTIC APPROACH TO SECURITY THAN EVER BEFORE. WHAT ARE THE MOST COMMON ATTACKS AGAINST THESE APPLICATIONS, AND HOW DOES IRDETO ACTIVECLOAK FOR MEDIA PROTECT YOU AGAINST THEM?

THE NEED FOR DIGITAL ASSET SECURITY

In the race to satisfy consumer demand for any time, any device consumption of video content, operators are challenged by the need to retain control over their distribution environments in order to meet licensing obligations for content security. As operators add support for popular consumer device and PC platforms such as Android, Apple iOS and Microsoft Windows, their exposure to piracy increases dramatically as these platforms are inherently less secure, leaving the content, especially downloaded content, in an environment where a hacker has full visibility and control over the executing code.

Commercial video and other digital content distributed over the Internet is often protected with DRM or other protection systems, where encrypted content files are sent from a content server to a client device or software. Thus, the DRM itself is often a target for attack, where hackers attempt to reverse-engineer code on the client device in order to discover keys and use them to decrypt the content. Once the DRM is circumvented, the digital content is free for unauthorized copying and use. Even when implemented using modern device-specific hardware security, DRM solutions are not able to withstand and recover from the attacks currently faced on today's increasingly open platforms.

ACTIVECLOAK™ FOR MEDIA

Is a dynamic security solution to protect and monetize high-value digital entertainment assets across a wide range of consumer devices. Launched in early 2011, ActiveCloak is based on Irdeto's renowned Cloakware technology, used in marquee solutions from leading digital entertainment companies such as Netflix, Comcast, Sony and Toshiba.

"...This is a real, bona fide breakthrough technique. It's also revolutionary, in that it starts with a bold statement for the DRM industry: an admission that it has a problem.

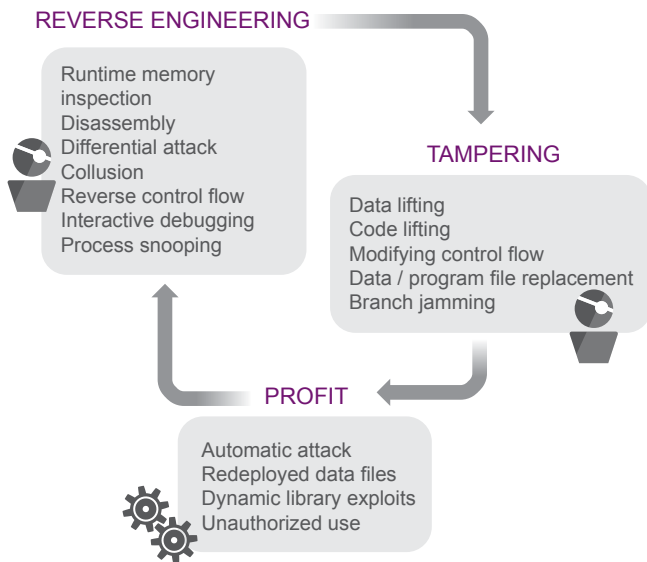
Now we have a product that embodies true synergies between the legacy Irdeto and Cloakware technologies. The system renews itself with respect to the key hiding and code hardening as well as the content protection itself, and it does so on a proactive basis. ActiveCloak gives new meaning to the term "race against the hackers": hackers must do their thing before the clock runs out and the system is renewed..."

Bill Rosenblatt - Giant Steps Media Technology Strategies

HACKER THREAT MODELS

Hackers intent on pirating content typically use one of two approaches to circumvent software-based protection mechanisms: they either attempt to reverse engineer the code to discover sensitive data such as cryptographic keys, certificates or resource files that will allow them to unlock the content, or they try to tamper with the code in order to modify its behavior to allow them access to the content. Depending on which approach they take, hackers use a variety of tools and techniques to carry out their attacks, and often collaborate with other hackers to multiply their efforts and increase their effectiveness and chance of success.

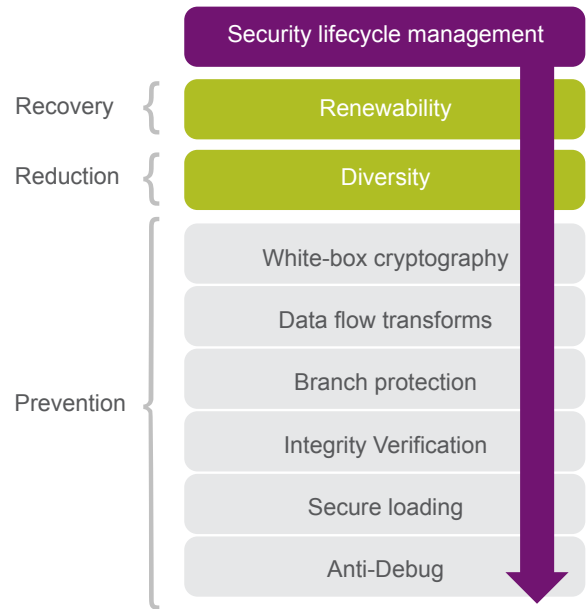
Whether motivated by profit, by ego or simply by the desire to watch licensed content for free, history has proven that, given enough time and resources, hackers will find a way to crack any protection mechanism placed in their path. The secret to defeating them is to make the task of breaking the security so difficult that it is no longer worth their effort to do so; in other words, to break the hacker business model.



Popular code hacking techniques used to reverse engineer and tamper with software

MULTIPLE LAYERS OF DEFENSE

The core technology behind Irdeto ActiveCloak for Media has long been considered by Hollywood studios and consumer electronics makers as the “gold standard” for software protection. Competing solutions often employ post-build, binary insertion techniques (e.g. guards), which by their very mechanics, can easily be removed by an adversary. What sets the Irdeto solution above and beyond other competing solutions is the compilation support for program transformations and obfuscation where the source code itself is transformed to hide control flow, data flow, usage, storage, etc. This provides a layered solution where binary and source-level protection techniques are combined to counter the widest variety of attack vectors.



This multi-layered defense strategy is further extended with software diversity and renewability to create an overall security lifecycle framework that focuses on the three pillars of dynamic security: attack prevention; threat reduction; and security recovery.

PREVENTION – STRONG INITIAL ATTACK RESISTANCE

The key to helping prevent attacks is to provide the strongest possible initial attack resistance. This is where Irdeto’s core Cloakware technology comes into play. Again using a technology layering approach, various software protection techniques are applied to the code in order to defeat or impede the progress of software pirates. Each of these techniques are designed to address different vulnerabilities with the application or code, and when used in combination, significantly increase the difficulty and skill level required in order to successfully reverse engineer or tamper with an application. When designing in these protections, often referred to as hardening the code, Irdeto engineers can pick and chose the most effective techniques based on the type of application being protected; this allow each solution to be custom tailored to the particular application to be protected in order to maximize the overall effectiveness of security.

Tools commonly used by hackers to reverse engineer and defeat DRM and other software protection systems

Debuggers	Allows hackers to step through the code being attacked, often bypassing common obfuscation methods
Decompilers	Used to convert binary code (machine language code) into source code which is easier to understand and manipulate
Disassemblers	Used to convert binary to a higher-level assembly language
Packet Sniffers	Used to intercept and log traffic passing over a digital network in order to analyze its contents

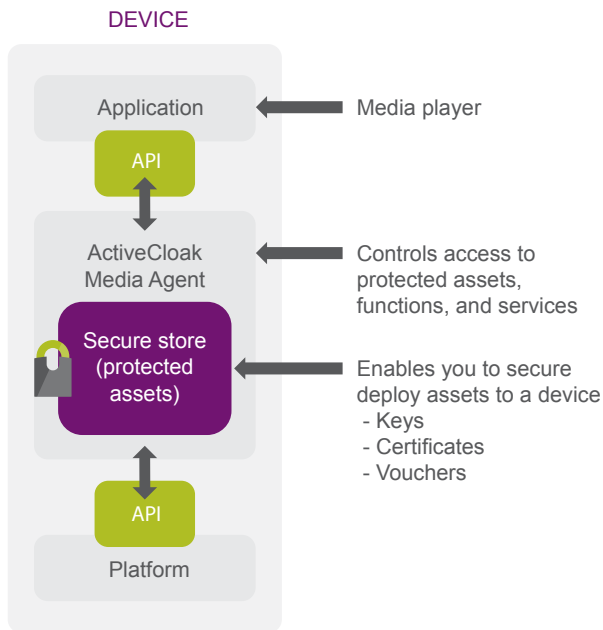
The following table lists examples of some of the software protection techniques used within ActiveCloak and the types of attacks they help prevent.

ActiveCloak protection technique	How it fights piracy
Anti-Debug	<ul style="list-style-type: none"> - Detects and prevents analysis of the application from a debugger
Branch Protection	<ul style="list-style-type: none"> - Protects conditional code branches from reverse engineering, tampering and exploitation - Prevents an attacker from forcing or “jamming” the condition in a certain direction
Control Flow Flattening	<ul style="list-style-type: none"> - Provides multiple control flow level settings and techniques - Allows programmers to strike a balance between security and right level of performance
Control Flow Transforms	<ul style="list-style-type: none"> - Hides original high-level control flow and highly structured control flow elements - Forces attacker to dynamically trace control flow
Data Flow Transforms	<ul style="list-style-type: none"> - Mathematical transformations that increase program complexity but retain original functionality - Makes reverse engineering, tampering, and exploitation more difficult
Function Signature Transforms	<ul style="list-style-type: none"> - Modifies function interfaces within a program to make all function calls identical in appearance - Makes it more difficult to identify the number, types, ordering, and values of the parameters and the return value of a protected function
Integrity Verification	<ul style="list-style-type: none"> - Verifies integrity of image and data files on disk and in memory
Node-locking	<ul style="list-style-type: none"> - Binds an application to an ActiveCloak agent running on a particular end-user device - Helps prevent host ID spoofing
Secure Loading	<ul style="list-style-type: none"> - Prevents static code analysis and tampering before module is loaded into memory
Security In-lining	<ul style="list-style-type: none"> - Extracts the body from a called function and combines it with the body from the “call site” - Removes the function call as an attack point
String Transforms	<ul style="list-style-type: none"> - Mathematical formulae applied to string literals - Conceal strings within final executable or dynamic library making human comprehension much more difficult
White-box Cryptography (Irdeto patented)	<ul style="list-style-type: none"> - Ensures that keys are not revealed while cryptographic computations are being observed in complete detail - Increases the difficulty of key extraction - Supports AES, RSA and ECC encryption algorithms

REDUCING PIRACY THREAT THROUGH SOFTWARE DIVERSITY

While strong initial attack resistance is critical to help delay attacks, ActiveCloak for Media takes security to the next level by limiting the impact of an eventual breach. Through software diversity, ActiveCloak ensures that only a small portion of the installed base will be affected by an attack.

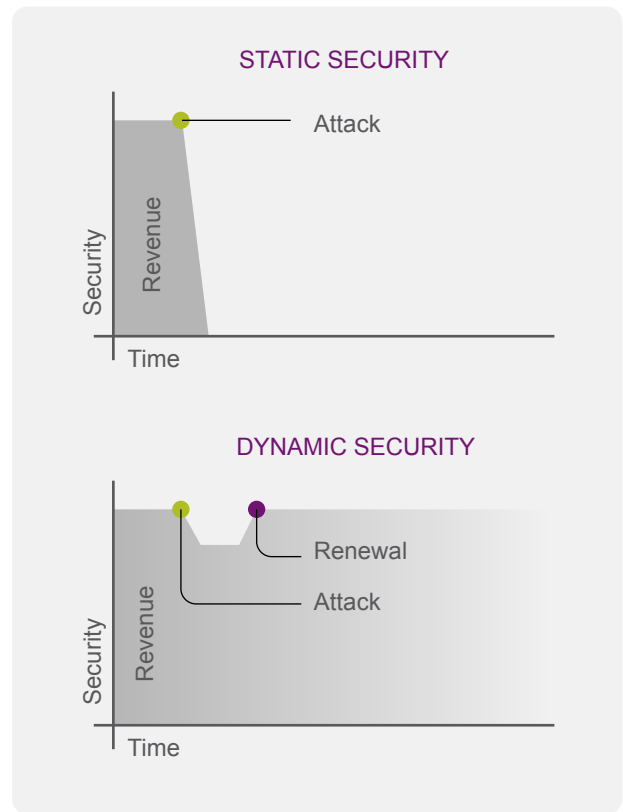
ActiveCloak automatically generates security “agents” that reside on client devices. By applying functionally equivalent but structurally diverse instances of these agents, ActiveCloak limits the impact of automated attacks, reducing both the financial exposure caused by the breach as well as the scope of deploying a corrective update. The flexibility of ActiveCloak allows diversity to be applied by device type, by software release, or even by individual subscriber. In contrast, hardware-based security solutions typically expose applications running on an entire device class, allowing hackers to package the attack as a tool to be shared and easily propagated.



ActiveCloak agents allow operators to control content security on their subscribers' devices

RENEWABLE SECURITY

Should an attack eventually be successful, renewing security to re-establish a secure environment is critical to limit prolonged exposure to content piracy. ActiveCloak allows operators to quickly renew the software agents already installed on client devices. This ability to renew its protection mechanisms is an important advantage of ActiveCloak for Media.



Potential revenue loss due to piracy is greatly reduced with security diversity and renewability

ActiveCloak core technology enables Irdeto's dynamic security model, the only security solution in the industry that combines the most advanced binary-level and source-level code protections, software diversity and security renewability to dramatically decrease the probability and ease of an attack while limiting the overall potential exposure during a specific attack. ActiveCloak dynamic security is the key to effective content protection.

ABOUT IRDETO

Irdeto is the most innovative software security and media technology company in the world. Through its dynamic security and monetization technologies, the company allows new forms of distribution for broadcast, broadband and mobile entertainment, and for the world's most popular app, eStores and consumer devices.

Co-headquartered in Amsterdam and Beijing, Irdeto employs 1000 people in 25 locations around the world. It is a subsidiary of broad-based media group Naspers.