



BindIT™

Securely node-lock software to preserve revenue

Secure Hardware Identification Prevents HostID Spoofing

Software publishers typically prevent uncontrolled copying of software by node-locking its license to a particular computer or license server. Node-locking is enforced by calculating a HostID that reflects unique characteristics of the computer, and tying this into the software license. At run time, the HostID in the license must be successfully matched against the host computer before the software is permitted to run.

If an arbitrary computer can be made to match the HostID, however, then this control strategy breaks down and uncontrolled piracy of the software is enabled. This attack is called HostID spoofing, and is particularly simple when weak characteristics such as the MAC are used to calculate the HostID. However, when implemented robustly, **node-locking** is the easiest way to recapture revenue lost to under-licensing.



Arxan's BindIT is a software-based node-locking solution which **combines strong resistance to HostID spoofing with low developer and customer impact**. Powered by Uniloc®, BindIT's patented device recognition algorithm combines numerous sampling points including hard drive damage maps, CPU and chip benchmarking, silicon degradation and damage, serial numbers, network structure, graphics, GUIDs and MAC addresses to generate a unique and highly spoof-proof computer fingerprint. This is then randomized to generate an alphanumeric HostID. The "tolerance" of a machine locked software activation system refers to the amount of change allowed in an enduser's PC before a re-authentication is required.

BindIT resists HostID spoofing in several layers:

- BindIT uses multiple unrelated factors, many of which are unique hardware-based patterns, making it practically impossible to set up or configure a second computer that matches the characteristics of the first.
- At run time, randomization and similar obfuscation strategies are used to make it very hard for a hacker to figure out how different factors are being used to compute the fingerprint, further reducing the likelihood that a successful HostID spoofing exploit can be generated.
- GuardIT, Arxan's comprehensive application hardening solution, can optionally be used to protect against tampering attacks to disable or bypass the node-locking functionality.

BindIT provides strong, performance efficient, cost effective and user-friendly node-locking for software applications. The result is reduced piracy, reduced technical support and development costs, and increased recapture of revenue from under-licensing.

How it Works

BindIT is added to your application in three simple steps:

Step 1 - At Development:

Add fingerprint logic to your software source

BindIT's fingerprint calculation and verification routines are supplied as a static library with SDK. During development time, add calls for this functionality to your C/C++ software application, or native component of your .NET or Java application, and link to the library – then compile as usual. You can also insert BindIT's fingerprint calculation routine into your software installation script. This allows the host machine's fingerprint to be calculated when the software is being installed, and for the HostID to be embedded into the license that is generated for the software.

Step 2 - After Compilation:

Optionally harden your compiled binary

BindIT includes one set of protections against reverse engineering and tampering. However, you can implement deeper and broader anti-tamper protection by additionally using GuardIT, a post-compilation application hardening tool. GuardIT includes a point-click protection feature to harden BindIT functionality in your application - Guards protect the computer fingerprinting component against reverse engineering, and tightly bind it with the software application to ensure the security functions cannot be separated, tampered with, or disabled. Alternatively, you can build a customized protection for your application structure and logic.

Step 3 - At Run Time:

Initiate and enforce node-locking

When your end user runs your protected application for the first time, either the installation script or the software application (depending on your design choice in Step 1) generates the computer's fingerprint and provides the HostID to your license management or node locking routine. This is stored for future reference, usually as part of the software license that is issued at installation. For each subsequent execution, the HostID is calculated from the host machine, and compared to the reference HostID. As long as there is a match, the software continues to run normally. If the match fails, a variety of reactions can be taken including phoning home with tampering information, allowing the software to run for a grace period, or restricting software features.

The Software Based Node-locking Advantage

Software based node locking offers significant benefits of low initial cost, high flexibility in terms of initial coding and ongoing updates, and the ability to sell software via an all-electronic online system. Historically the main drawback to software based host identification schemes has been the ease with which they can be spoofed or bypassed.

Traditionally, software publishers have used hardware dongles that plug into the end user's serial cable slot or USB to node lock. This requires that the hardware dongle be present at the license server or the end user computer for the software to run, which makes for a cumbersome and intrusive end-user experience, and a higher cost of ownership. What's more, many internet services offer dongle cloning in "24 hours or less, guaranteed", which makes this option less secure than Arxan's software based solution.

Arxan's secure software based solution:

- 1. Delivers a lower TCO for software publishers.** Publishers incur lower initial costs in acquiring and deploying the dongles, as well as lower ongoing maintenance and support costs since there is no hardware-like risk in the dongles getting lost or simply failing.
- 2. Lower TCO for the end customer as well.** Dongles are unpopular with end users, who often choose to use a pirated version of the software rather than deal with the cumbersome nature of the dongle. With our software based solution, end customers incur lower costs since they do not need to maintain, track and replace dongles.
- 3. Security that is comparable to, and often higher than that of hardware dongles.** Through a combination of multi-factor fingerprinting at the algorithmic level, seamless integration into the software, and sophisticated obfuscation and encryption at the binary level, Arxan's secure binding solution enables security without the cost and inconvenience of hardware dongles.

Features and Benefits of BindIT

Feature	Benefit
Device Recognition	BindIT uniquely fingerprints a computer based on multiple hardware and software characteristics, to provide a HostID which enables node-locking
Integration with license management	BindIT provides point-click integration of node locking logic with FLEXnet Publisher. It also supports interoperability with any license management or online activation system.
Tolerance	By allowing some system characteristics to change before a re-authentication is required, normal customer upgrades and normal computer wear-and-tear can be accommodated without disrupting user experience or incurring expensive technical support calls. (Tolerance is tunable, and non-tolerant operation is also supported.)

Advantages of BindIT

- **Easy to Use** – BindIT's simple API enables fast and error-free integration and deployment. The API is fully customizable for power users.
- **Customer Friendly** – BindIT's fingerprint comparison routine allows a small number of component changes before a mismatch is reported, ensuring that minor system upgrades don't create expensive support calls and annoy customers. Intolerant operation, where no changes are allowed, is also supported.
- **Algorithmically Strong** - BindIT's patented approach to computer fingerprinting is fundamentally secure and resistant to spoofing. Many different computer characteristics, ranging from hardware flaw patterns to system configuration, are used to generate the HostID. It is very hard to spoof these multiple factors simultaneously.
- **Spoof-Proof** – The hardware fingerprint is based on multiple factors, including some which are intrinsic to the hardware and are practically impossible to replicate on another computer. There is no obvious mapping between hardware details and the 156 character HostID. The fingerprint is also randomized, to further hinder reverse engineering.

Complementary Arxan Technologies

The Arxan product suite includes the following offerings which complement BindIT in fully securing software against piracy and unauthorized use:

- **GuardIT** provides comprehensive application hardening to protect the overall software package against reverse engineering and tampering.
- **GuardIT for FLEXnet Publisher (FNP)** provides point-click hardening of applications using this popular license management solution from Acresso®. BindIT and GuardIT for FNP work seamlessly together to integrate the HostID into the FNP license, and enforce the node locking at run-time.
- **Remote Notify** is a powerful solution to discover under-licensing and recapture low-hanging revenue. Notification is activated if the computed HostID fails to match the ID in the license, and reports back offender information for rapid follow up by your sales or product management team.
- **TransformIT** is a white box cryptography (WBC) solution which can mesh the HostID and a secret key into an overall cryptographic decryption routine. Critical parts of the binary are encrypted, with the decryption key protected via WBC and hooked with the HostID, to provide highly intricate hardware binding.

About Arxan

Arxan Technologies Inc. is a leading provider of application hardening solutions designed to protect software applications from tampering to minimize risk and maximize profitability. Our advanced software protection solutions secure enterprises, ISVs and digital media providers against unauthorized use, malware insertion, piracy, and reverse engineering of intellectual property. Our products defend, detect, alert and react to attacks through a threat-based, customizable approach that is proven, easy to use and non-disruptive. Arxan supports a full range of application protection needs, from commercial software to military grade assurance. The government relies on ADS Systems to deliver a best-of-breed anti-tamper platform to protect critical program information. Founded in 2001, Arxan Technologies has offices in Bethesda, MD, San Francisco, CA and West Lafayette, IN. For more information, please visit www.arxan.com.

