Software Piracy: How to Protect Your Software Assets

Stay ahead of the curve

Mike Dager
CEO, Arxan Technologies
11.13.07
Software Piracy Losses

1. **FACT**: 35% of software revenues are lost to piracy each year (*on average*)

2. **FACT**: Software piracy growing at 20% a year

3. **FACT**: $41 billion lost in 2006 globally to software piracy

*Software applications are unprotected!*

*Source: Third Annual BSA and IDC Global Software Piracy Study, May 2007*

Software Piracy: Rampant

Two-thirds of software, costing $200B, will be pirated over next 5 years

Hackers bypassing Symantec; trying to use their software tools as actual gateway into corporate servers

“Chinese pirates busted with $500 million of software”

“Microsoft’s DRM Hacked”

“Licensees inadvertently neglected to encrypt the decryption key “

“Successful iPhone Hack”

“EDA-Software vendors are taking software protection seriously”

“The Next Piracy Panic: Software”

“Software piracy a booming Net trade”

“Huawei lifted... software code” from Cisco router

“China Sets Sights on Machine Tool Development”

Stay ahead of the curve
2006 Piracy Rates by Country

Piracy Rate: the percentage of software installed in a country without a license.

Top 3 Regions:
- APAC: 68%
- CEU: 68%
- Latin Am: 66%

35% avg

Source: Third Annual BSA and IDC Global Software Piracy Study, May 2007; Note: APAC region avg excludes Japan, Australia and New Zealand.
Less Piracy = More Revenue

Microsoft Reports Strong Gain on Sales of PC and Server Software

“Mr. Liddell (Microsoft CFO) also said the company’s efforts to combat piracy were particularly successful, increasing sales of some product lines by as much as 5 percent from a year earlier.

‘It’s only one quarter, so we’re not getting carried away here,” Mr. Liddell said, “but the anti-piracy really helped.’”

New York Times, 10/26/07

Shares hit highest levels since mid-2001

"While upside from solid PC growth and the 'Halo 3' launch were relatively expected, further upside came from improved piracy rates and uptake of premium server editions," analysts at Thomas Weisel Partners wrote in a note Friday.

Marketwatch, 10/26/07
Software Piracy Websites

Stay ahead of the curve

Arxan Confidential
# Software Piracy Websites

Stay ahead of the curve

![CrackSpider.net](image1.png)

![HackZone.us](image2.png)

![eMule](image3.png)

<table>
<thead>
<tr>
<th>File Name</th>
<th>Size</th>
<th>Sources</th>
<th>Type</th>
<th>File ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>version 13 cracks.exe</td>
<td>29 KB</td>
<td>67 (67)</td>
<td>Programs</td>
<td>98643D7CA894D90A09243F905A5CFDA0</td>
</tr>
<tr>
<td>AutoCAD v13.0 - Enterprise Edition + Crack.iso</td>
<td>339.76 MB</td>
<td>27 (26)</td>
<td>CD-Image</td>
<td>5913A8D10F51395A12A2698BF2D2A9AF14</td>
</tr>
<tr>
<td><img src="image4.png" alt="SoftSummit" /></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Arxan Confidential
About Arxan Technologies

- **Our Mission:** protect software applications, stem the $40B lost to global piracy each year

- **Our Offering:** application hardening solutions, designed to protect software IP from piracy, tampering and reverse engineering.

- Focused on enterprise ISVs and software application vendors
- State of the art Guard™ technology
  - Arxan security becoming a standard within the DoD
- Grew revenues more than 100% per year for last 3 years
- Offices in Bethesda, Indiana, San Francisco, Dallas, Boston, Chicago, Huntsville and New York

Stay ahead of the curve
Hacking Defined

• **Piracy**: make unauthorized copies of proprietary software and sell reproductions at bargain prices, thereby stealing revenue from the organization creating the software.

• **Tampering**: alter proprietary software to give access to others or enhance the software's functionality. Users might seek to add features, delete restrictions or to access hidden functionality.

• **Reverse Engineering**: extract code in order to steal intellectual property, confidential information, and proprietary algorithms.

• **Insertion of Exploits**: insert viruses or other malware into pirated versions.
Hacking Tools and Techniques

*Common desktop SW exploits, in increasing order of difficulty:*

- **Determine method to generate valid keys**
  - Reverse engineer key creation or find keys that can be reused
- **Spoof the presence of valid licenses**
  - For example, by cloning a license server
- **Bypass license management**
  - Tamper with decision making routines
  - Eliminate decision making routines altogether
- **Fully reverse engineer product**
  - Extract IP-rich routines and package into a counterfeit product

*Software applications are unprotected!*
Arxan Technologies

Arxan protects software IP from piracy, tampering, reverse engineering, and any manner of theft.

- Our patented technology includes, but goes beyond obfuscation and encryption to actively protect software

- We defend, detect, and react to attempted attacks through a layered and dynamic network of Guards™ to provide defense-in-depth
  - Continuous addition of Guard types in anticipation and reaction to new hacking / pirating techniques

- Proven: Dept of Defense pedigree since 2001; successfully hardening commercial applications with millions of lines of code
Arxan Protection Process

- Standard SDLC: software is unprotected from piracy, tampering and theft.
- Protected-SDLC with GuardIT: Arxan easily integrates protection into the SDLC.

<table>
<thead>
<tr>
<th>SDLC</th>
<th>ARXAN PROTECTION</th>
<th>FINAL QA</th>
<th>DEPLOYMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>DESIGN</td>
<td>STEP 1</td>
<td>Assess Risk</td>
<td></td>
</tr>
<tr>
<td>DEVELOP</td>
<td>STEP 2</td>
<td>GuardScript Design Wizard with the option to modify the GuardScript</td>
<td></td>
</tr>
<tr>
<td>COMPILE</td>
<td>STEP 3</td>
<td>GuardIT Insertion Engine</td>
<td></td>
</tr>
<tr>
<td>TEST</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Arxan Protection Technology

- **Defend** against compromise
  - Encryption and Obfuscation to deter static reverse engineering
    - Including powerful white box cryptography for key protection
  - Pre- and post-damage to minimize window of opportunity

- **Detect** attempted attacks
  - Anti-Debug to detect reverse engineering attempts
  - Authentication and anti-tamper to detect modification attempts

- **React** to ward off attack
  - Self-healing to undo attempted tampering
  - Customizable reactions, e.g. traitor tracing, warn user, exit or crash

- **Implemented as Guards**
  - Small security units, under 100 instructions each
  - Inserted directly into the binary by sophisticated engine
  - Guard the application and each other, in deep intricate layers
Guard™ Technology: Intelligent Software Protection

Guards: security units injected into binary to protect key functions and cover risks

- Easy to use
  - Automated insertion of protection

- Durable & Resilient
  - Network of Guards, so no single point of failure
  - Surgical, precise placement of Guards

- Dynamic
  - Defend, detect and react to threats

- Transparent to application and to SDLC
  - Binary-based technology dissolves in
  - No changes to source-code
“Moving Maze” Architecture
Arxan Protects Across Threat Spectrum

Level of Protection

Arxan

Obfuscation Tools

Encryption

Wrappers

Attacker Profile

Regular User

Script Kiddie

Amateur Pirate

Professional Pirate

Organized Nation-State Team

Stay ahead of the curve
How Arxan Application Protection Works

Unprotected Application Structure

Protected Application Structure (Orange = Guard)

Activation Init
Node locking Init
LM Init

Application

Main Program Image

Activation functions
Node locking functions
LM functions
The Result…

- Resilient
- Durable
- Development Friendly
- Dynamic
- Easy to Use
- Low Performance Impact
- Proven

© Arxan Technologies 2007
7 Reasons to Choose Arxan…

1. Dynamic
   > Dynamic Guards complement static obfuscation and encryption to detect attacks and react to overcome threat

2. Durable
   > Interconnected mesh structure removes single points of failure. Additional measures like diversification and randomized security prevent construction of reliable BORE exploit

3. Resilient
   > Protection easily reconfigured and rapidly reapplied to quickly respond to potential breaches
   > Protection easily enhanced to account for evolving threatosphere

4. Development Friendly
   > Binary-based solution does not disrupt coding process or schedule
   > Debugging tools ensure QA process is not disrupted
   > Does not affect SDLC
...and ship your product with confidence

5. Easy to Use
   > Intuitive interface to quickly build customized protection scheme
   > Command line interface to integrate protection into build scripts
   > Guard insertion and diversification is fully automated

6. Proven
   > Protection technology has been stress tested through existing deployments and stringent third party testing
   > Arxan constantly evolves Guard technology, keeping you one step ahead of hackers

7. Low Performance Impact
   > Minimal run-time performance impact – no speed/coverage tradeoff
   > Security does not invade end-user system
   > Minimal interference with field debugging and customer support
Stay ahead of the curve

Use Cases

Preventing Software Piracy and Tampering
### User Story: Desktop Software Vendor

<table>
<thead>
<tr>
<th><strong>SW Vendor Goal</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sell sophisticated oil field modeling software with million-dollar range license fees, to countries with high piracy rates and no legal or government IP protection.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>SW Vendor Problem</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>License management and dongle security mechanisms being easily hacked</td>
<td></td>
</tr>
<tr>
<td>Hacked version of new releases available via cracked SW sites within days of GA</td>
<td></td>
</tr>
<tr>
<td>Complex application, many exploitable gaps between modules</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Arxan Solution</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Full risk assessment, then complete fortification of application with Arxan</td>
<td></td>
</tr>
<tr>
<td>Protected application passed rigorous 3-week external red team testing</td>
<td></td>
</tr>
<tr>
<td><strong>Arxan now being deployed enterprise-wide by SW Vendor for 6 months and not hacked</strong></td>
<td></td>
</tr>
</tbody>
</table>

Stay ahead of the curve
Customer Case Study: Media Gateway Provider

- **Customer:**
  - Digital media gateway company
  - High-end home media server and VoIP boxes sold via distribution channel with subscription services

- **Customer Goals:**
  - Secure software application in media gateway from theft
  - Protect VoIP application client from tampering
  - Ensure that subsidized box will not be unlocked
  - Keep digital media safe

- **Arxan Solution**
  - Prevent tampering and reverse engineering through Guard technology
  - Trusted boot chain and secure node locking of software to media gateway device chipset (Linux on PowerPC)
Customer Case Study: IPTV Platform

• Customer:
  > IPTV streaming company
  > Streams free or subsidized TV programming to PCs with custom advertisement insertion

• Customer Goals:
  > Keep digital media safe
  > Secure software application against reverse engineering
  > Ensure client cannot be tampered to remove or bypass advertisements

• Arxan Solution
  > Prevent tampering and reverse engineering via Guard technology
  > Ensure protection is not only durable but also easily renewable
  > Secure PC software without impacting real-time performance requirements
Customer Case Study: Machine Tool Co.

- **Customer Challenge**
  
  - Prevent software piracy, loss of revenue
  - Had seen product illegally sold on internet
  - Protect software-based IP in sensitive metal shaping algorithms
    - Business shifting from HW to SW

- **Arxan’s Solution**
  
  - Team did vulnerability assessment
  - Customer asked Arxan to try and hack their software
  - Arxan then protected machine with Guard technology

"Within 90 minutes of submitting them our code, they had an illegal version operating. That to me showed expertise and credibility."

"They’re able to insert these objects in your code with so many levels of nesting that it becomes almost impossible from a time or resource perspective to be able to break through them"
User Story: Navy

- Navy Goals
  - Protect Key IP

- Navy Problem
  - Export to foreign country was multi year process of proving that battle mgmt. software could not be “enhanced” to US version levels

- Arxan Solution
  - Protect key routines from modification, reverse engineering or code lifting
  - Force return to depot for maintenance if tamper detected
Stay ahead of the curve

Special Guest:

Mr. Tommy Miller
Product Development Manager
Schlumberger
Thank You

Please contact us at info@arxan.com