State of the Practice of Software Anti-Tamper

Capt David Chaboya
Air Force Research Labs
Anti-Tamper and Software Protection Initiative (AT-SPI) Technology Office
20 Jun 2007
Introduction

• AT-SPI Background
• Understanding the RE Threat
• Software Protection Techniques
• Protection Case Studies
• Software Protection Vendors
• Conclusion
Software Protection Initiative (SPI)

- **Goal:** Protect critical DoD application software (running on general purpose computers) from piracy and exploitation
- **Lead:** DUSD(S&T)
  - **Office of Primary Responsibility (OPR):** AFRL AT-SPI Technology Office

Scientific & Engineering/Modeling & Simulation Software

Mission Support Software

Enterprise Software containing critical personnel, pay, or medical information
Mission
Anti-Tamper Software Protection Office

- To deter the reverse engineering (RE) and exploitation of our military’s critical technology…..

- AC130U
  - ~609,000 source lines of code (SLOC)

- F-22
  - ~2 million SLOC

- JSF
  - ~19 million SLOC
Reverse Engineering

Intellectual Property

```assembly
; 000015A 833B00  cmp dword ptr [esi], 00000000
; 000015D 0F8412FF77FF je 00000075
; 0000159 80C604  add esi, 00000004
; 0000155 013E20646147 cmp dword ptr [esi], 47616420
; 000015C 7419  je 00000187
; 000015E 3906  cmp dword ptr [esi], eax
; 0000160 74C0  je 0000017C
; 0000162 331E  cmp dword ptr [esi], ebx
; 0000164 0F84FBFF77FF je 00000075
; 000016A 3BE7  jmp 00000153

\[
TMF = \left\{ \frac{\int_0^5 f^3 A(f) \, df}{\int_0^5 A(f) \, df} \right\}^{\frac{1}{3}}
\]
```
Commercial Piracy

- Business Software Alliance (BSA) – 2006 Global Software Piracy Study
  - 35% of software installed worldwide illegal
  - $34 billion in pirated software

- Commercial companies seek to limit initial piracy/reverse engineering
Commercial Piracy
Consumer Education

Garret the Ferret
-Copyright Crusader

RE Threat

• Access
• Analysis
• Understanding
Tools of the Trade
Static Analysis

- Decompilers
  - Boomerang
  - IDAPro beta plugin

- Disassemblers
  - IDAPro
Tools of the Trade
Dynamic Analysis

- Debuggers
  - Ollydbg
  - WinDbg
  - VAMPiRE
  - Hardware ICE

- Emulators
  - Bochs
  - Custom Virtualizers
Software Protection Techniques

- Hardware Storage/Processing
- Obfuscation
- Anti-debugging
- Encryption
- Checksums
- Diversity
Software Anti-Tamper (AT)

- Two major types in industry
  - Encryption wrappers
  - Integrated protections

Source: http://www.slane.co.nz/cartoons.html  
Source: www.6seconds.org/anabel/map.html
Protections: Why they Fail

• Causes problems for the end user
• Negatively impacts performance
• Opens security holes
• Tedious to apply
• Easily broken
  – BORE attacks
Starforce Case Study

- $5 Million dollar lawsuit claiming software DRM was insecure
- Users claimed StarForce causes computer instability and crashes

Ubisoft officially dumps Starforce

Citing "complaints," the publisher ends its relationship with the copyright-protection provider.

By Tor Thorsen, GameSpot
Posted Apr 13, 2006 5:56 pm PT

Following several days of rumors, Ubisoft has officially confirmed that it will no longer use the controversial digital-rights software from Starforce.

Sony XCP
Case Study

- Sony BMG music CDs shipped with copy protection scheme
- Protection installs system driver that hides any file or process that begins with $sys$
- Protection device driver left system open to privilege escalation attack
AACS Case Study

- Advanced Access Content System
  - Copy protection
  - Modification/Decryption protection
  - Renewability and revocation

- Encryption only protects data at rest
  - Code (e.g., keys) visible upon execution
XProtector Case Study

- Software protection focused on kernel mode driver
- Discontinued due to repeated published breaks
- Updated product renamed as Themida
- Protection transitioned from kernel module to Virtual Machine
Ideal Software Protection

- High level of security against best attackers
- Low performance impact
- Resistant to repeat/automated attacks
- Protects against all forms of runtime analysis
- Securely locks to hardware
- Easy to apply
Protection Process

1. Determine Critical Information
2. Assess the Threat
3. Create Protection Plan
4. Implement Test Deploy
5. Monitor and Sustain
Metrics

• Difficult questions
  – How much protection is enough?
  – How long will it last?

• Determining metrics
  – Blackhat assessments
  – Red teams
  – Markets
  – Formal modeling
Sample of Protection Vendors

- Arxan

- Pikewerks
  - http://www.pikewerks.com/research.htm

- Cloakware
  - http://www.cloakware.com/products_services/security_suite/

- Luna
  - http://www.lunainnovations.com/research/secure.htm
Conclusion

- Software Protection (AT) is still very much in its infancy
- Significant research into formalizing protection techniques and assessment metrics
- Autonomous and dynamic/polymorphic protections will improve and become more prevalent
- Increased support from hardware (e.g., TPM) and software (e.g., Microsoft) vendors for secure systems
Capt David Chaboya
Air Force Research Labs
Anti-Tamper and Software Protection Initiative (AT-SPI) Technology Office
Email: david.chaboya@wpafbc.af.mil
Phone: 937-320-9068
Acronyms

- AACS - Advanced Access Content System
- AFRL – Air Force Research Labs
- AT – Anti Tamper
- BORE – Break Once Run Everywhere
- DRM – Digital Rights Management
- DUSD(S&T) – Deputy Undersecretary of Defense (Science and Technology)
- OPR – Office of Primary Responsibility
- RE – Reverse Engineering
- SLOC – Source Lines of Code
- SPI – Software Protection Initiative
- TPM – Trusted Platform Module