Designing and Attacking DRM

Nate Lawson | Root Labs | 2008/4/11 | Session Code: HT1-402



If you pay attention, you'll learn...

- Why software protection matters
- Attack methods
 - Tools & techniques
- Design principles
 - Model: mesh vs. chain
 - Anti-debugging is no panacea
- Update: who's cracked or not



My background

- Root Labs founder
 - Design and analyze security schemes
 - Emphasis on embedded, kernel, software protection, and crypto
- IBM/ISS
 - Original developer of RealSecure IDS
- Cryptography Research
 - Co-designed Blu-ray disc content protection layer, aka BD+



In the past, DRM was simple

- Copy protection (1980's) lacksquare
 - Simple goal: only run from the original floppy media
 - No privacy problems
 - Relatively harmless

oot labs

- Some games did format themselves if not properly cracked
- Legal restrictions only via copyright, not on analyzing schemes or releasing tools





Today, bad DRM is too common

- Goals overly complex
 - Can share among a few devices but not too many
 - Expiration dates, limited number of plays
- Privacy problems
 - Network access
 - Cookies
- Collateral damage when it goes bad
- Dangerous and unclear legal environment
- If there's going to be DRM, make it simpler!



Definition: software protection

- Software protection is the technical enforcement mechanism
 - DRM is the policy, a different talk
- Composed from:
 - Integrity protection
 - Obfuscation/anti-debugging
 - Encryption/key management
 - Renewability



Why you will care



Laptop disk encryption

- Common myth: software protection only matters for DRM
- Nope!
 - "Cold Boot Attacks on Encryption Keys", Halderman et al
 - Extract FileVault key from RAM after a reboot
 - Or, freeze RAM with cold spray and move to another computer
- If you use software encryption, you need effective obfuscation
 - Since the key is somewhere in RAM, key hiding vital
 - Exactly same problem as DRM



Exploit protection

- If you want to make exploits difficult, obfuscate
 - Address layout randomization
 - Initial stack configuration
 - Future: compilers will randomize code generation
- Integrity checking
 - Stack canaries
 - Vista PatchGuard (aka Kernel Patch Protection)
- Same measures as DRM



Malware analysis

- Malware hides with same techniques as DRM
 - But worse!
- DRM designers have the harder problem
 - "Do no harm"
 - Debuggers must be allowed for legitimate work
 - No persistent modifications
 - Avoid interfering with Vista PatchGuard
- All these areas require knowledge of the same techniques
 as designing or analyzing DRM

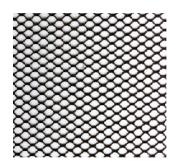


Designing software protection



Software protection design principles

- Mesh vs. chain
 - Protection measures should be mutually enforcing
 - Example: two threads hashing each other
 - A chain is a long series of links
 - Failure of any one link and it falls apart
- Full integration with application functions
 - Protection must be intertwined with main functionality
- Renewability
 - Provide yourself a way to repair hacks





Integrity protection

- Goal: respond to modifications
 - Explicit: detect and perform some action
 - Implicit: modifications directly cause change
- Many things can perturb the environment
 - Patching
 - INT3 breakpoints
 - Attaching debugger
- Implicit integrity protection better than explicit
 - Check/response are not separable logic
 - Prevent "divide-and-conquer"





Obfuscation/anti-debugging



- Goal: make inspection more difficult
 - Obfuscation: logic becomes harder to understand or patch coherently
 - Anti-debugging: respond to the act of inspecting the program
- Better if mixed with integrity protection
 - Example: hash the results of various anti-debugging checks and use as key to decrypt next function
- Most anti-debugging is poorly-implemented
 - Single point checks with if/then logic

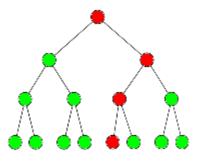


RSACONFERENCE2008

Encryption/key management

- Encryption in software protection is a type of obfuscation
 - Cipher+key in some form present in memory
- Key management
 - Broadcast encryption
 - Encrypt content key with lots of keys
 - Stop doing this for known-hacked keys
 - Software protection can make this more versatile
 - "You must be at least this unhacked to decrypt the video"





Renewability



- Every scheme needs a survival plan
- Online updates
 - Common in a PC environment
 - Caveats: version roll-back, privacy
- Piggy-backing on content
 - Better in embedded/cross-platform environments
 - Caveat: heterogeneity complicates testing
 - Examples
 - DTV/Dish send updates in channel stream ("ECMs")
 - BD+ puts protection logic on each Blu-ray disc



Tools & techniques



Historical reverser's toolbag

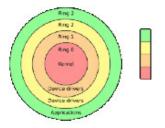
- In the past
 - debug.exe
 - SoftICE with iceext
 - IDA Pro doing static disassembly
 - Hex editor
- Today
 - IDA, Ollydbg
 - Bindiff, binnavi
 - Paimei
 - Custom tools







Tip: go to ring 0



- Even if you're attacking a user-mode app, kernel access gives a powerful viewpoint
 - Full access to thread state
 - No modification of process memory (i.e., int3 instruction)
 - Access to page protection, MSRs, etc. allow stealth schemes
- More advanced
 - Patch bochs/qemu
 - Write your own hypervisor debug stub



WinDbg is awesome

- Powerful tool for reversing
 - Kernel and usermode access
 - Automatic symbol server
 - x86 32 and 64-bit support
 - Extensions for common tasks ("!peb")
 - Open plug-in interface
 - Free
- Downsides
 - No third-party CPU extensions (sorry ARM)
- Let's make it the next SoftICE

이 가지는 대표한 데 비면에서 한 민준이는 것이다. 또한 제 봐				
 projvenoste normer under entre principal de la 		ткакатыну		
Another (6, "General event provided that the District of the 2%)		OTIVE:		Presiduo Neix
1		example as include		with the stand
1011 (C. 1010)		CONTRACT MODEWOOD	2 1	A 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4
referre fy		ENDOUTS T MO		17314
		ADDITION TO THE	per l	
ACTER DREPARTMENT OF STRATCHER AND A MARKET AND A DREAM A DREAM AND AND A DREAM AND A DREAM AND A DREAM AND AND A DREAM AND AND A DREAM AND		60/17161 Dec2	100	[rest (s.T]) and
ENVELONG CONTRACTOR		ENDINE INTER	10 A	ACC. SECHICL
		ADDITION WOULD IN CO.	- 10 Miles	(1) The Completion of the state of the sector state of the Completion of the state of the sector
LENGTON CLEVICE FROM A DE L'ANTI CAVER RECENTER CONTRACTOR		\$5/171 1 1945av		Income Million
 despire dim drafdeper maxig = 1, dim al, di p 				 Contractory and the state of th
CONTROL IN MILE AND ADDRESS OF		CONTRACT A CONTRACT	201 04 104	ended in the state of the second seco
		60/17110_004546		Jane - Collection (Collection)
emilting (4)- And Emile (244ms(541ms))		PRODUCT PROFILE	In the second second	CHARLES TRANSPORTER CONTRACTOR AND INCOME. 2014.
		CONTROL 10400	200	and and
		CONTRACT DATA	- S	Terraria and the second second
flash of a Thirp		0012102.2411		CERCIPTION FOR THE PROPERTY AND A DESCRIPTION OF
7	E	CONTRACT INCOME.		and taby total
edentationadarapp Clearingsongs		(4)		
AN IOF /	<u>80</u> 21	10756		
- press of the second state of the second s		ground Innatores		
And the second development development development and the second sec		New	Sec. 1	
414 (M1 (S22) 1177 112		NACION 1		
N 2014 - y Narod 2000 (a), ekseminist 2000 (and external anti-databased (anti-databased), saked 2010 (a).		strends.	:	
alge67/17/instarge1e17ab75 uige67/iur01 for ind to the set of all the residence		1.001		
THE D THERE PERCENT THERE AVER ATTRACT		L desitor	121001111	CALCULARY
rich Freid 2010 (1997) Bern By Libers (2010) - State (2010) Million and Freidinger (2010) - Charles Made State (2010) - State	100	E SECON		 CLASS, STOCK PRODUCTS, SECTORS
bietde p		- arcan	(500011)	
ALCHARACHAR ANNA AR ANNA ANNA ANNA ANNA ANNA ANN		1 105		e Recents and delegations of t
which which denotes another second details		LATER DATE: 1		en en en en deux de la companya de la
siz fundi di Martin sing Swarfar da Santa (1923) Ni kata da Santa (1931) na sina kata da Kata (1923) na santa (1920) nga sata (1931) na sina kata (1931) na sina		1 0.11572/16005		CHARTER IN THE REPORT
and the second		a with a rought		CONTRACTOR AND A CONTRACTOR
	14	11	1.194	and the second se
4 : mr:/	100	Looph Colb		



Tip: use debug registers creatively

- Intel processors have hardware breakpoints
 - DR0-3: addresses to be monitored
 - DR6: status bits that describe which event occurred
 - DR7: configures the type of event to monitor for each address
- Interesting side effects
 - DR4-5 are aliases for DR6-7 if the CR4.DE bit is clear
 - DR7.GD bit causes reads or writes to any of the debug registers to generate an INT1
 - Legacy behavior from ICE days



Update on recent hacks





000



iTunes 8

Ś

Dependence (Marcola, Marcola, Marcola, Sona, Appleare the Apple regions material of Apple regions of the Apple reg

MPG1 an Saulo integration options of Practices for a 104005 margined a

CD and mano-mained care from Graphics CCDOS, mayning: \$2000, 2000 Graphics Graphics Collection Software, converting, 2000-2003 Creations, The product.

Recent hacks this year

- Nintendo Wii
 - Loader compromised (tmbinc; Dec)
 - Software save game hack (bushing, segher, tmbinc; Feb)
- Windows Media DRM
 - drmdbg decrypts keys and is staying current with updates (Jan)
- iTunes
 - requiem decrypter released, removed via C&D (Feb)
 - Tools that rip audio samples from memory still exist (QTFairUse6, myFairTunes7)
- iPhone
 - Bootloader software compromise (iPhone Dev Team; March)



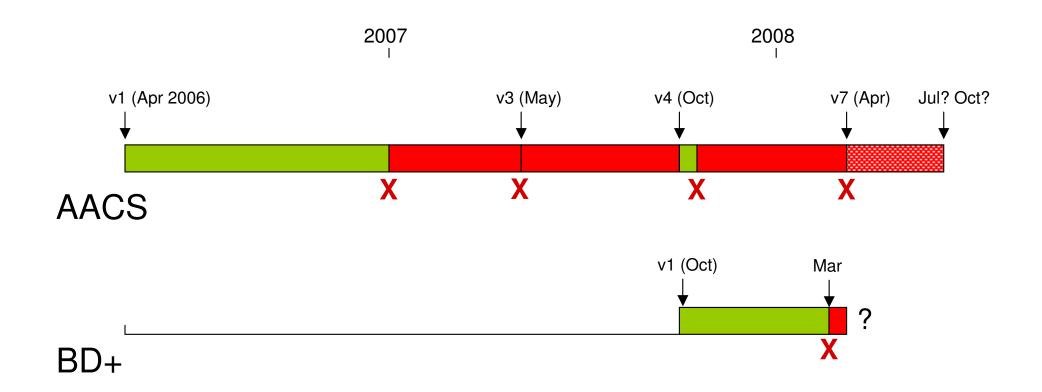
AACS vs. BD+

- Both allow updates to security
 - AACS: new MKBs and player keys
 - BD+: new software on discs
- Effectiveness metrics
 - How long each update survives before being hacked (L)
 - How frequently the updates appear (T)
 - If L < T, you are releasing new discs into an already-hacked environment!
- Goal: increase L, decrease T





Timeline of hacks





RSACONFERENCE2008

AACS analysis

• Not doing so hot



- Very low L (length of time update is unbroken)
 - -2 ... +2 weeks if you throw out the initial period
 - Long T (time between updates)
 - < 3 months not allowed by business agreements
 - Up to 18 months if hacked player not identified
 - Appears to be steady now at every 6 months
- Game over or ...?
 - Unmasking the Slysoft oracle
 - Sequence keys



BD+ analysis

- Too early to tell
- Flexible L



- Software protection can be a small or large barrier, depending on effort invested
- Potentially lower T
 - Update schedule in hands of disc authors
 - Potentially less parties to coordinate with for updates
 - Just test and ship a disc
- 2008 will be an exciting year!



Questions?

For more on software protection, check out my blog "rdist" at: rootlabs.com

