Cracking at Scale
KansasFest 2017
Presented by Mark Pilgrim
Notes by Jeremy Barr-Hyde

14:30-15:30

Thursday 20 July 2017

https://www.youtube.com/watch?v=KzLGC6Tz1Pc

6hr 06 min in

Revised 25-26/07/2017 with input from presenter and reviewing the presentation.

14:30 Joke: Where does the cracker throw all his dirty bits when company comes over? Under DESYNC! *Tough crowd.*

14:32 Cracking math blaster
Bootloader is encrypted with a one byte key and *every* disk is different! Capture the decrypted version.
Find the Weakbits protection check nestled in between the regular disk reading code. This reads track 0 sector 0, address epilogue twice and makes sure it's different every time. This was a fun trick used by many different protection schemes to ensure that the storage medium returns random data. Sounds insane.
Rotating address prologues different on every track. Normalise that!
Different nibble translation table… just slightly different - normalise.
RWTS swapper to accommodate save game and data disc – side 2. Disable.
Disk volume number is 000 which is literally impossible to create with standard tools. Checked at runtime, repeatedly!

A BASIC program changes its environment and re-runs itself to reveal a new BASIC program! Which then changes its own environment *again*, e.g. changing the Applesoft program area.

The second level changes environment again and runs itself again. Third level changes and then program run. And it checks for volume number 000 again.

Embedded serial numbers - erase!

The entire DOS system is compatible with 3.3 but all entry points are shifted 2 bytes to the left. Essentially producing thousands of points for later copy protection checks. So, if you get through ALL of that, you get... Math Blaster! *Still no clapping?*

So, what if you wrote a program to do all of that? Mark explains step by step the patches while referring to an example Passport log on slide. From that you get *Overview of the Bible (1983)*. And you get   From this other programs such as the Bingo Bugglebee series (1985) and *Grasshopper Dissection* in 1990 (7 years on). Audience comment: *Grasshopper Dissection? Sounds like a metal band name!*

And Ultimo IV uses the same protection - *now I have your attention*.

Trivia: First to be de-protected? Ultima IV. Lead way for preservation of the previously mentioned titles. And we see this pattern over and over again.

If you can crack Spanish Achievement 1, you have Spanish Achievement 1. If you can automate that routine with a program, you then get English Achievement 1. Joke: It’s a little involved (Mark referring to a slide showing complex patches). Not others of course - it’s copy protection. Ardy the Aardvark, Datamost, splash screen on show (with appropriate composite CRT filter applied). You can conclude the original cracker of Ardy the Aardvark did not go back and crack Flash Spell Helicopter (1983) when he or she was done.

Cracking Ernie’s Quiz
You get Ernie’s Quiz.
Shout out to Catherine (not present).
But Passport allows for further cracking of very early educational and productivity software. Titles include Instant Zoo (1981); Letter Man (1982) and Shopping with the Yellow Pages (1984). Apple themselves created this copy protection and licensed it to publishers. A range of titles are shown on slide.   Magic Spells (1981) published by Advanced Learning Technologies, later rebranded to The Learning Company who went on to published Rocky’s boots and many more. The Speed Reader (1981) was the very first program by Jan Davidson, who later founded Davidson & Associates. Her doctorate was in American Studies; she was a teacher.

Elite, D. Braben (1985). Space simulation/strategy game with 3D wire framing and *exactly* the same protection as Ernie’s Quiz.

Mark: Passport has improved since the last time I was here and presented in 2016. It now has a universal Activision patcher, courtesy of Brian Troha (present for applause).

All of these big-name Activision games such as Shanghai, Rocky Horror Show; you find the common protection code then you can crack all these games (list of titles shown). Including *How to Weigh an Elephant*, Litag… for free! That isn't an Activision product. So that copy protection was productised, and that version was then offered to other companies.

Disk duplication houses may have had a business of licensing protection routines. These didn't stay in house necessarily.

Electronic arts are famous for their virtual machines and interpretative language, then wrote the CP in that language… if you get a universal patcher from Qkumba, thank you, that can crack movie Maker. We did a lot of construction in the 80s - Bards Tale leads to…. Financial Cookbook by EA! A short-lived attempt of EA's in the 80s. They wrote a processor called cut and paste, which had the exact protection from Bard's Tale. Guess what was cracked first?

Trivia: Qkumba has been very busy.

Anti-tamper checks - Nibble 14 minutes in.
Mr Cool is a cool Qbert clone. Apple Cider Spider

Trivia: Sammy Lightfoot favourite game of 4ams.

Slide: Passport

This is all now in passport. It's an automatic disk verification and copy program. I'm back to Kfest to announce it has been under active development over the past 371 days.

Universal patching incorporates Activision as we know but other routines such as $BBF9 desync. John Brooks submitted his title 'Tomahawk' for de-protection. This isn't the only title to be self-presented.

Gamco did games like Capitalization. Used Beagle compiler, poked a bad block check into memory then called it. It was fun! *Actual* fun may vary.

Self-destructing MECC disks - one thing they'd do is a master disk and then a limited boot backup which counts each use. 50 uses? I'm sorry you've booted this too many times, disk catalogue trashed along with data. master Disks were supposed to be mailed back to MECC. unlike modern software distribution where it takes seconds, it would have taken weeks for a replacement. Nasty. Passport takes care of this.

Fixes - SO MANY. Scholastic' Grolier - edge cases. Passport can notify of ProDOS RWTS variants regardless of patches applied or not.   This surfaced more information which goes beyond cracking. Fundamentally a verification program and data miner. The raw material, the ore with diamond pick axe, … wait scratch that - too much Minecraft…

Passport is surfacing information about these disks that may or not be readily obvious. Things like third party DOSen. Apple DOS 3.3 was very slow so a market sprung up - diversiDOS. Shareware $30…. Mark didn’t pay.

A lot of educational programs used a real file system, except it was prontoDOS or diversiDOS. This is where these DOSen products made money.

All of this is new from the past year.

The upcoming release that was released in May, ready for download. Upcoming features are RAM Disk support - hardware supported include GS Ram disks, RamFast. Disks ready to memory, patched, written out.   Exciting to take advantage of memory expansion. Again, thank you to Qkumba for development on this new feature.

The original version of passport (released at KFest 2016) was written and assembled in Merlin programming language. Now we have migrated to modern laptops for editing, assembling (open source software Acme).

Mark suggests github.com/a2-4am/passport for the code, welcomes contribution. Still runs on A][+ ć 64kb. RAM disk use is automatic.

2016 brought the announcement of 42 unpreserved disks being cracked by Passport. The past year has brought a total of titles 542! And of those, many are preserved for the first time – 425!

At Passport's heart is a verification tool. Initially written to verify .EDD images that were made from collections. OpenEmulator //e by Zellyn Hunter can boot them, sure. But if a sector related to level 7 was corrupt, gameplay could not be guaranteed.

Automation; OE and Passport run with log file captured automatically.

Link: archive.org/download/VogonLaundromat
*Hitchhikers guide to the galaxy reference.

Technical anthropology

What can you do with 4000 verified EDD disk images? AND the resulting .DSK images sans protection? And the .TXT file of the passport log?

This dataset proves that:
202 $E7 bit streams desynchronising check.
163 LSR $6A
see side for further
138 $DE + timing
13 JMP ($BBDE) - this page is later overwritten and moved.

This isn't 202 disks from the same company, it's from dozens of companies. Grolier, Sunburst, Troll (and more) all used and re-used protection that's what Passport targets.

What can't be done? Yes, it'll be a Chess program (Qkumba, a grand master cracker) has spent hours on this). A lot of one offs (in the removal of protection) which deep dives into new routines.

protection is a valued added thing bought from duplication houses. E.G Troll's Tale has two different versions and subsequent protection. helps beat Copy II plus for example.

Question posed about buying copy protection versus developing it in-house.
Answer: Mark was 11. His work is better than talking to someone about history (joke) but welcomes discussion on this topic.

John Brooks presents facts: Datasoft was in three groups. Disk duplication, development and warehouse (for physical distribution). Mid to late 80s where not all shops had access to copy protection tech, and customised duplication schemes that can do it…. Those that did were sought out... Those being companies that can also store and ship the product post duplication.

Mark: Copy protection is hard and has trade-offs. The programming required is very different in comparison to the game development itself. Broderbund had in house. Sirius too.

Reminder that this was a cat and mouse game - months after product release would bring a new version of Copy II Plus. Forcing expensive redevelopment of software.

A summary of DOSen used by publishing houses is shown, numbers showing the protection is built on top of the DOS. One is pronto-DOS which puts code on an unused part of Pronto-DOS which is used in other third party DOSen.

Trends, statistics and popularity can be summarised from the past year's data mining.

A tale of two trolls (and so many sticky bears) appear identical in physical media. Booting, identical. Protection? Completely different. Someone had to have revised the game, leading to new protection. This complicates preservation when versions are different yet unlabelled.

Logs that are expected to be the same, but aren't, is where the identification of these titles show up.

Sticky Bear is notorious for identical physical presentation yet protection routines applied to the same title can change up to four unique times.

Opportunities in future preservation workflows: Extraction, derivation, aggregation, investigation.

Before dinner time today, someone could build a tool to extract Applesoft source from a range of discs and save it to text file.

A hacked version of MECC's copy program lead the way to a 32mb disk image, hard drive bootable of these titles. 40-50 titles per 32mb compilation.

Empowering users to make their own compilations of titles previously not hard drive bootable.

Cultural anthropology - take The Learning Company. Watch them progress through looking at early titles and seeing their progression as programming skills mature. Dr Leslie M Grimm of TLC used a then age 11 Corrine Grimm for in game artwork. Mark notes he can see the quality of artwork progress as Corrine gets older.

Mark: I don't wonder anymore if this is worth doing. I don't argue who think everything is preserved or judge what is worthwhile. I've seen what is rotting away on physical media.
MECC's database on Soviet Union, which fell in 1991.
And Squgies's book on drugs! Alcohol bad, vaccines good.

These are not just bits, disks, artefacts. They are curriculum. Kids USED this in the 80s. Especially considering MECC was single platform.

Last but not least.

(60L TUB is placed on the desk). Mar: This is about 600 MECC disks - I can personally guarantee each is imaged. I have checked the version numbers, checked gameplay, EDD imaged them and archived them. Then verified them with passport, then uploaded them to Archive.org. They are yours. PLEASE take them - and would someone help me carry them up (for garage giveaway).

Joke: Did you hear that honey? (toward the camera) - THEY ARE NOT coming home!

And last finally; I'm going to press C.

A demonstration, in less than 30 seconds' completion, shows Ultima IV Origins being deprotected in *Passport*. Patches are applied in real-time to serial numbers, RWTS and more. A disk image is written to slot 5 drive 1 to a USB stick with a CFFA3000.

(mark goes to menu selection).

Ultima IV, origin, loads instantly.

Question: Who is 4AM?
Answer: I don't know!