

השתרשות אנדרואיד: מדריך למפתחים

דבר ראשון - זה לא על איך להחיל שיטת השתרשות, למשל, שורש בלחיצה אחת, על מכשיר אנדרואיד. במקום זאת, מדובר על איך אפשר ללכת לפיתוח שיטת רוטציה למכשיר שאף אחד לא עשה רוט לפני כן, והוא מסופר דרך ההתנסויות שלי עם Barnes & Noble Nook - שורש מכשיר מסוים - ה Table 8GB. להקשר, אתה יכול לקרוא את ["Root for Nook Tablet 8GB"](#) [השרשור המקורי שלי](#) XDA-Developers [ב-Android Market \(עם 8GB\)](#) שבו פרסמתי את שיטת ההשרשה שלי, שהגיעה לספירת הורדות של - חכה לזה - מעל תשע אלפים!!!

לסקירה כללית של איך ההשרשה עובדת מאחורי הקלעים, מומלץ לקרוא את המאמר הקודם שלי [איך ההשרשה עובדת - הסבר טכני של תהליך ההשתרשות באנדרואיד](#) כרקע.

מתישהו בסוף פברואר (2012), בביקור בחנות Nook-בארנס אנד נובל בבוסטון, קניתי את ה Table 8GB שזה עתה יצא לאור, לגמרי בדחף Table 8GB שאני, הדבר hax0r-תמורת 199 דולר. בהיותי הראשון שעשיתי כשהגעתי הביתה היה לנסות להרוס את המכשיר. זאת הייתה הפתעה לא נעימה, אם כן, כשגיליתי שאף אחד עדיין לא הצליח להשריש את המכשיר. כל מה שהצלחתי למצוא זה [סרטון יוטיוב](#) שמראה ששיטת ההשרשה הקיימת לא עבדה. Nook Tablet 16GB-עבור בן דודו, ה לאחר המתנה של כמה ימים, חנות האפליקציות

צ'ואן ג'י



על אודות

פרויקטים

מאמרים

הערות טכניות



צ'ואן ג'י



על אודות

פרויקטים

מאמרים

הערות טכניות

הניעו B&N הפתטית לחלוטין והמוגבלות שהקים אותי סוף סוף לפתח שיטת השתרשות למכשיר בעצמי.

התוכנית

אז איך עושים שורש מכשיר אנדרואיד? כפי שהסברתי במאמר [הקודם שלי](#), השתרשות היא בעצם תהליך דו-שלבי:

- מצא ניצול המאפשר ביצוע של קוד שרירותי. כשורש
- עם סט (su כדי להתקין exploit-השתמש ב. Superuser.apk ו-root SUID) סיביות

כהלכה, Superuser.apk התקנתם su לאחר Titanium כגון) אפליקציות הדורשות שורש להפעיל קוד su יפעילו (AdAway או Backup כמשתמש הרשאי.

התהליך

יש הרבה ניצולים גנריים או ספציפיים למכשיר ש עשוי למנוף כדי להשיג ביצוע מיוחס של קוד hax0r שרירותי. אפנה אותך שוב למצגת [המצוינת הזו על ניצול שורשי אנדרואיד שונים](#) ששימשו או עשויים לשמש למטרה זו.

עם זאת, אף אחת מהשיטות האלה שהכרתי לא שהוא כנראה, Nook Tablet-יכולה לעבוד על ה: האנדרואיד הנעולים ביותר שיש ROMs-אחד מ

- טוען האתחול נעול.
- מושבת ולא ניתן להפעיל אותו ADB מהממשק.



צ'ואן ג'י



על אודות

פרויקטים

מאמרים

הערות טכניות

- חבילות) התקנת אפליקציות שאינן בשוק מושבתת, ולא ניתן להפעיל (גולמיות APK אותה מהממשק
- Google Play / Android-אין גישה ל Market (או כל Google Apps).

זה שולל 1) חבילות שורש ו-2) את רוב הניצולות זה אומר שאי ADB שדורשות ביצוע פקודות על אפשר להריץ שום קוד על המכשיר שלא מגיע מתקופת B&N.

אבל כמובן שהייתה דרך אחרת להיכנס. מישהו ב-Gילה שמטען האתחול של ה XDA-Developers תומך באתחול של מערכת אנדרואיד Nook Tablet הממוקמת בתמונות מחיצות המאוחסנות בכרטיס חיצוני. מנגנון זה משמש כנראה לתיקון microSD מחיצות מערכת פגומות על ידי תמיכת לקוחות של B&N.

הפתרון, אם כן, ברור: אנו יוצרים תמונות מחיצות מערכת דמה שבמקום לאתחל מערכת אנדרואיד, את מערכת Superuser.apk ומתקין su מתקינות האנדרואיד ה"רגילה" בזיכרון פלאש פנימי. באופן קונקרטי יותר, שיניתי את קובץ אתחול המערכת שבתמונת מחיצת האתחול כדי להפעיל initrd בתוך סקריפט מותאם אישית שהעתיק את הקבצים בזיכרון הפלאש system הרלוונטיים למחיצה הפנימי.

של ndubootביססתי את עבודתי על תמונות 2

כדי לפרוק bootimg-והשתמשתי ב bauwks

: boot.img קבצים בתמונת מחיצת האתחול

```
# Extracts files in the boot partition
image into the current directory.
bootimg -x ./boot.img
# Extract files in the initrd cpio arc
hive into the folder ./ramdisk/
boot-unpack-initrd ./initrd.img
```



צ'ואן ג'י



על אודות

פרויקטים

מאמרים

הערות טכניות



שיניתי את קובץ אתחול המערכת

כדי להעלות את `initrd` ב-`omap4430.rc`

מחיצת המערכת של זיכרון ההבזק הפנימי במקום

מכיוון ששלבי אתחול המערכת, `/system` ב-`/foo`

מאוחרים יותר מנסים לטעון מחדש

כקריאה בלבד וכן הלאה, ומשום מה לא `/system`

:יכולתי לבטל את ההתנהגות הזו

```
on fs
    mkdir /foo
    mount ext4 /dev/block/platform/mmc
i-omap-hs.1/by-name/system /foo wait
```

הוספתי את הדברים הבאים לקובץ אתחול

כדי להתחיל את `initrd` ב-`init.rc` המערכת

:סקריפט ההרשה שלי

```
service root_script /sbin/busybox ash
/assets/run.sh
oneshot
```

סקריפט ההרשה שלי, שאני מציב בספרייה

אלא גם את, `su` מתקין לא רק, ב-`initrd` `assets`

ואפליקציות אחרות של גוגל Google Play

Nook Tablet ROM-שחסרות ב

```
# Install su and Superuser.apk
/sbin/busybox cp /assets/su /foo/bin/
/sbin/busybox cp /assets/su /foo/sbin/
/sbin/busybox chmod 06755 /foo/sbin/su
/sbin/busybox chmod 06755 /foo/bin/su
/sbin/busybox cp /assets/Superuser.apk
/foo/app/
```

```
# Install Busybox.
/sbin/busybox cp /sbin/busybox /foo/xbin/
in/
/sbin/busybox chmod 06755 /foo/xbin/bu
sybox
```

```
# Install Google Play and other Google
apps.
/sbin/busybox cp /assets/*.apk /foo/ap
```

צ'ואן ג'י



על אודות

פרויקטים

מאמרים

הערות טכניות

```
p/  
/sbin/busybox cp /assets/com.google.android.maps.xml /foo/etc/permissions/  
/sbin/busybox cp /assets/com.google.android.maps.jar /foo/framework/  
/sbin/busybox cp /assets/libvoicerecognition.so /foo/lib/
```

```
# Done.
```

```
/sbin/busybox mount -o ro,remount /foo
```

בהתאם לסקריפט שלמעלה, שמתי את כל הנכסים Busybox-ואת ה-initrd בתוך ה-assets בספרייה עם כל השינויים ה-initrd ה-sbin הבינארי בתוך boot.img שבוצעו, אני אורז הכל בחזרה לתוך חדש:

```
# Build initrd cpio archive  
abootimg-pack-initrd initrd.img.new  
# Build new boot.img using previously  
extracted components  
abootimg --create boot.img.new -f ./bootimg.cfg -k ./zImage -r ./initrd.img.new
```

תמונת כרטיס boot.img לאחר מכן אני מחליף את ושיטת, boot.img.new בתמונה שלי של SD-הההשרשה מתבצעת.

מילים אחרונות

התהליך בפועל, כמובן, היה הרבה הרבה יותר ברך Nook Tablet-כואב. מאתר האתחול של ה פשוט לא יעבדו, microSD-מאוד; חלק מכרטיסי ה וכו'. גם לאחר boot.img יש מגבלת גודל קובץ ב /foo trick-mount-to- תסכול רב גיליתי את ה ולא יכולתי אפילו לעקוב אחר כמה שחזורי יצרן הייתי צריך לבצע במכשיר כדי לבטל שינויים גרועים. אבל זה עדיין היה מאוד כיף, ואי אפשר להפריז באופוריה בסוף ובתחושת ההישג



כשהתחילו להתגלגל הודעות תשובות ואנשים
אקראיים תרמו 5 דולר כאות להערכתם

בהצלחה השתרשות!

וייל

בוק

טר

למקדאין

טאמבלר



פנטרסט

צ'ואן ג'י



על אודות

פרויקטים

מאמרים

הערות טכניות

ALSO ON JICHU4N.COM

10 years ago · 13 comments

**How X Window
Managers Work,
And ...**

8 years ago · 1 con

**Unicode I/C
Locales in I**

צ'ואן ג'י



על אודות

פרויקטים

מאמרים

הערות טכניות



15 Comments

 Login

Join the discussion...

LOG IN WITH






OR SIGN UP WITH DISQUS ?



Name

 5 [Share](#)

[Best](#) [Newest](#) [Oldest](#)

J [John Hammer](#)  
6 years ago
This is cool and inspiring. Thanks for the write up.

31 0 [Reply](#) 

M [Misty Zhu](#)  
10 years ago
This is so cool! Thank you so much!

I have a question: I see you mount the system at /foo, then copy su and superuser.apk to the subdir. But to root a device you need to place su and superuser.apk under /system subdir. How does those two files transport from /foo to /system?

25 0 [Reply](#) 

[Chuan Ji](#) Mod  

 [Misty Zhu](#)

10 years ago

During the rooting process, I mount the system partition at /foo, so when I'm copying these files to /foo, I'm actually writing them to the system partition.

When the device restarts

צ'ואן ג'י



על אודות

פרויקטים

מאמרים

הערות טכניות

when the device restarts normally afterwards, it will mount the system partition at /system, so whatever I wrote to the system partition perviously will just show up.

See explanation of mounting here:

<http://unix.stackexchange.c...>

0 0 Reply ↗

A

Aldrich

11 years ago

Thank you for sharing this.

3 0 Reply ↗

M

minusfrogs

3 years ago

I know its been a long time now, and thats good for my question, have you found out a better way to the testing process? Like a vm that can help speedup the factory reset or something like that, or do you have to have the hardware? Also why dont you have a twitter?

0 0 Reply ↗

Vinod Cs

3 years ago

very nice article...beautifully explained the details of rooting

0 0 Reply ↗

Filipe Welington

3 years ago

Nice Article Thanks for share!

0 0 Reply ↗

D

Duater

4 years ago

Can someone how to do this for vivo y15s

0 0 Reply ↗

P

Pramodh Rachuri

5 years ago



צ'ואן ג'י



על אודות

פרויקטים

מאמרים

הערות טכניות

I am in 2019 and still reading your 2011 article. I actually got into to this page after reading <http://jichu4n.com/posts/ho...> Very well written and clear. Good job man!

0 0 Reply ↗

Darío

7 years ago

I wanted to thank you for encouraging me to keep trying. Your method didn't work for me (I didn't manage to run a script from init.rc), but I did modify mounting permissions and so from the init files so I could place the binaries I needed from a common adb shell, once I owned /system and some subfolders. It took me days of trying, giving up and trying again next day. But finally I rooted it. Shamefully, I must confess, I was more encouraged by the process rather than rooting itself, though now I can free some space up and chill around with some stuff.

0 0 Reply ↗

S

Shaikq

7 years ago

this is interesting :)

0 0 Reply ↗

Jin Freaks

9 years ago

Oh, I also have a question or two, how and when that script will be executed? It seems it'll be executed at boot cause you include it to the kernel? Am I correct?

0 0 Reply ↗

© 2024 Chuan Ji. כל הזכויות שמורות.

