Ardrand: Arduino sem vélbúnaðar slembitölugjafi
Post Mortem

Benedikt Kristinsson
Leiðbeinandi: Ýmir Vigfússon

Desember 2011

1 Upphafleg áætlun

Upphaflega stóð ég í þeirri trú að það væri hægt að nota Arduino sem einfaldan slembigjafa án mikillar fyrirhafnar. Áætlunin var að fyrst freina gögn úr örtölvuni og síðan búa til slembitölugjafa með henni. Endanlegur afurður átti að vera forritseining fyrir Linux-kjarnan til þess að bæta slembni við `/dev/random` og `/dev/urandom`. Það reyndist hinsvegar erfitt að fá slembni út úr Arduino og þessi afurður kom aldrei til skjalana.

1.1 Tímaplan

Í byrjun verkefnis skrifaði ég niður verkþætti og áætlað tímaplan fyrir hvern þeirra. Það var eftirfarandi

Ritrýni/Lit. review ca 100 tímar. Skrifa úrdrætti úr greinum og byggja upp lista af heimildum.

Tilraunir ca 120 tímar. Búa til upphaflegar tilraunir og tölfræðilegar prófanir án þess að fá endanlegar niðurstöður strax.

Framkvæmd Skrifa umrædda forritseiningu fyrir Linux kjarnan. Framkvæma tölfræðilegar prófanir með endanlegum niðurstöðum.

2 Raunveruleg framkvæmd

Fyrstu vikurnar fóru í það að lesa greinar og skrifa úrdrætti. Ég byggði upp safn af úrdráttum inn á Google Docs sem deilt var með leiðbeinanda. Einnig las ég viðeigandi kafla í Schneier bókini „Applied Cryptography" og í Menezes bókini „Handbook of Applied Cryptography". Sumar greinar reyndust mjög torlesnar, skemmst er að minnast á að ég var viku að lesa grein eftir U.M. Mauer — svo var mér tjáð að hann væri þungur í lestri.

2.1 Breyting á stefnu verkefnis

Eftir að hafa byggt upp ágætis safn af greinum fór ég að skoða niðurstöður úr Arduino. Örtölvan Arduino hefur analog-til-digital breytir og hugmyndin var sú að nota suð í þessum breyti til þess að lesa slembin gildi[1] með fallinu `analogRead` á Arduino. Það kom fljótt í ljós að ekki væri hægt að lesa gildin „hrá" og nýta sem slembni. Hinsvegar þá hafa framleiðendur Arduino mælt með að nota úrkomu úr þessu falli sem sæði/fræ fyrir PRNG. Þá breyttist stefna verkefnisns í að sýna fram á að þessi staðhæfing væri röng.

Til þess að sýna fram á veikleika umræddar staðhæfingar skrifaði ég forrit sem tekur runu frá PRNG úr `avr-libc` (notað af Arduino) og finnur sæðið sem notað var.

2.2 Vandamál sem komu upp

Þegar ég var að prufa útkomur við mismunandi aðstæður og hita setti ég einn Arduino inn í frystir yfir nótt. Þegar ég tók hann út morgunin eftir var hann ónýtur og hættur að svara. Arduino hafa ekki gefið út upplýsingar um hitastig fyrir vélbúnaðinn en AVR, fyrirtækið sem framleiðir örgjörvan, hafa gefið út að hann þoli allt að $-35°$C. Fyrstirinn var u.þ.b. $-11°$ C.

Það kom einnig í ljós að umhverfisáhrifin voru mikil og undir lok verkefnis fundust tölvur og aðstæður þar sem Arduino gat framleitt slembnar tölur með aðferðum sem lýstar eru í rannsóknarskýrslu. Þetti olli að ég þrufti að gera breytingar á lokaskýrslu á óheppilegum tíma, en engu að síður var það afar ánægulegt að hafa tekist að framleiða tölur sem virðast slembnar. Þetta kom töluvert á óvart.

2.3 Hvað lærði nemandinn?

Ég lærði um uppbyggingu á slembiföllum og -vélbúnaði, þá bæði pseudo-slembiföllum og raunverulegri slembni. Einnig kynntist ég hvernig Linux PRNG virkar (`/dev/random`).

Ég fékk praktíska reynslu á beitingu tölfræði við greiningu gagna. Það má til gamans geta að ég sá hagnýtan tilgang í erfðum klösum við forritun verkefinsins, en það er eitthvað sem ég tel vera kennt á rangan hátt í skólum. Ég notaði git[2] við umhald og sýslu á öllum mínum forritskóða og kynntist því betur.

En það sem ég tel mig hafa grætt mest á er að hafa kynnst hvernig það er að vinna sjálfstætt að rannsóknarverkefni frá upphafi til enda, að undanskildum fjárveitingum. Ég lagði fram þessa hugmynd sjálfur og starfaði meir eða minna sjálfstætt við framkvæmd verkefnins, þó ég gat alltaf leitað til Kristján Vals, doktorsnema við HR og Ýmis, leiðbeinanda míns. Þetta tel ég hafa verið verðmæt reynsla.

3 Tími

Þar sem stefna verkefnins breyttist töluvert þá stóðst upphaflegt tímaplan ekki alveg. Ekki var fylgst nákvæmlega með tímanotkun en áætlaður tími fyrir þá verkþætti sem framkvæmdir voru er eitthvað í samræmi við

[1] Sjá rannsóknarskýrslu fyrir nánari útskýringu

[2] `http://www.git-scm.com`

Ritrýni 110 tímar. Að lesa greinar og skrifa úrdrætti reyndist tímafrekara en ég hafði gert ráð fyrir

Tilraunir og tölfræðilegar prófanir 200 tímar. Ég framkvæmdi bæði greiningu á „hráum" gögnum sem og tölfræðiprófanir. Þessir tveir verkþættir tvinnuðust meira eða minna saman og erfitt er að gera upp um hve miklum tíma var eytt í hvorn. Ég forritaði tölfræðiprófin sjálfur og aðferðir til þess að reyna að finna slembni á Arduino.

Skýrslugerð 90 tímar. Mér gekk vonum framar að skrifa lokaskýrsluna og vinna að henni, þó að það hafi vissulega tvinnast saman við tölfræðilegar prófanir og aðrar tilraunir. Það hljálpaði mikið að hafa skrifað góða úrdrætti úr lesnum greinum.