one laptop per child

security

agenda

- what are we protecting?
- how are we doing it?
- system security vs. anti-theft
- open questions: content filtering, infrastructure
- what's new

security for olpc means six core things

prevent hardware damage by software

provide recoverability and openness (learner's machine) prevent permanent data loss

protect the user's privacy

prevent the laptops from being a platform for attacks keep the laptop under control of its owner

goals

no user passwords

out of the box security

open design

no reading

no lockdown

difficulties.

current systems just don't do this.

they rely on users making sensible, informed decisions on things they don't understand.

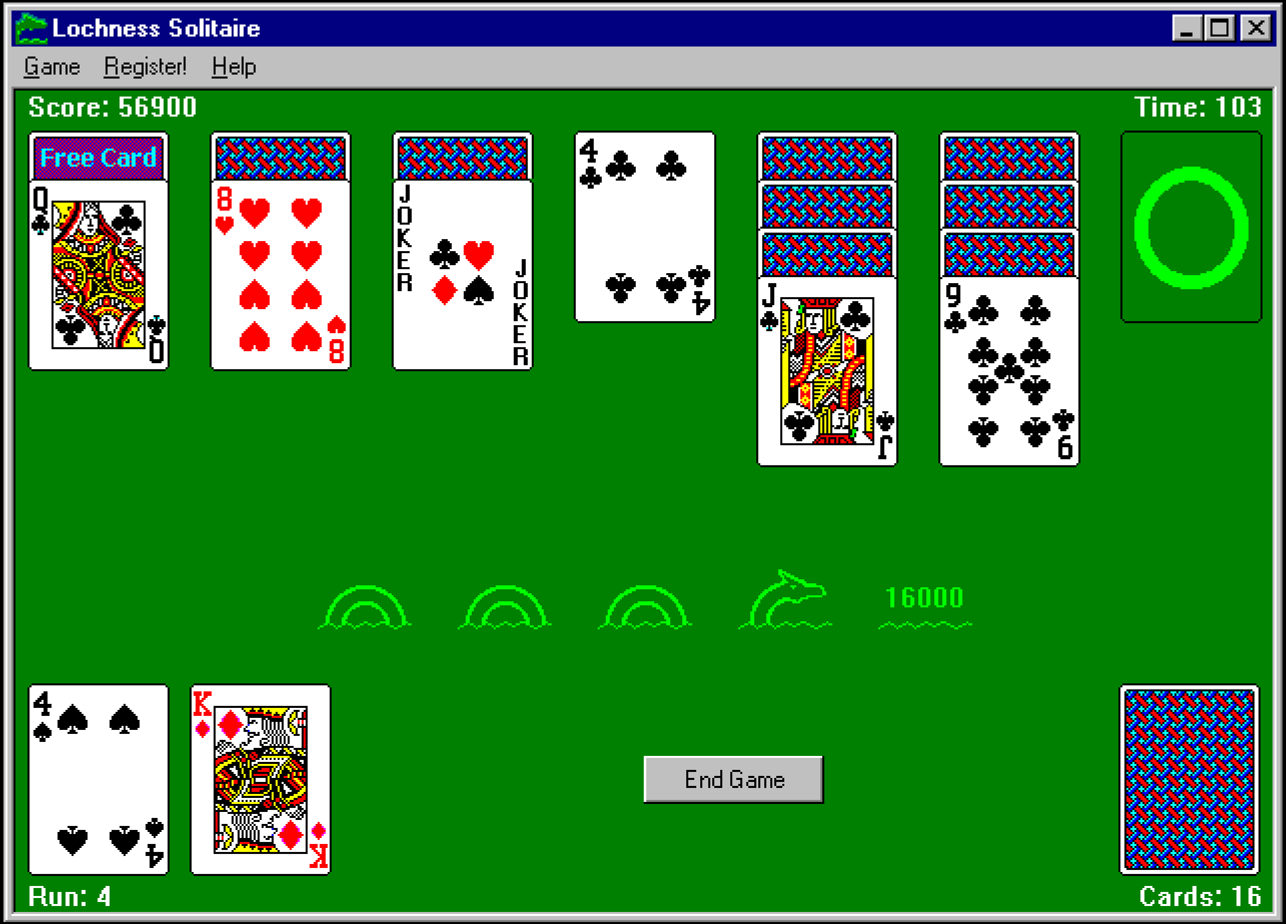
example: the very dangerous program

can: delete your hard drive, corrupt or erase all your documens or send them to russia, read your e-mail, impersonate you…

can: spy on you with your microphone and camera, let someone else control your computer fully…

guesses?

solitaire.



Score: 56900

Time: 103

Run: 4

Cards: 16

we designed a new platform called bitfrost.

attempts to satisfy all the preceding goals.

main idea: run each application in its own virtual machine.

give each program only the permissions it needs.

with this approach, viruses and spyware just “go away”.

hardware damage can be prevented.

recoverability: can restore full factory system data loss: mitigated by revisioning and easy backups

privacy: microphone
and camera LEDs,
explicit user action
to access documents

preventing use as an attack platform: connection limiting, throttling, automatic packet shaping will it work?

already works in prototype testing.

completed a round of expert peer review. no design issues identified.

bitfrost core ready to be merged in our kernels, blocking on higher-priority work.

there's a bunch of userspace software to be written.

target: C-test

several open questions before then

i talked about
system security

two more matters: anti-theft/activation and content filtering

1. cryptographic leases and activation

not at all infallible,
but reasonably
strong deterrent

2. objectionable content filtering

olpc doesn't want to be in that business update and anti-theft infrastructure: centralized at OLPC in the beginning getting the infrastructure security wrong is a nuclear check mate

what's new?

we can radically simplify the initial anti-theft system moving from leases to 'active disable' system.

system armed but inactive: we can use it if need arises, but don't have to do full logistics up front but still have to figure out activation logistics. more complicated if offline.

discussion:

- activation
- simpler anti-theft
- content filtering
- questions?