Assessing software protection effectiveness: Experiments with students

Cataldo Basile
< cataldo.basile @ polito.it >

Politecnico di Torino
Dip. Automatica e Informatica

Software needs effective protection

software contains valuable assets
- **billions lost every year**
- **company and user security at stake**

software protections mitigate risks
- **several techniques proposed in literature**
- **different level of effectiveness**

```
int E,L,O,R,G[42][m],h[2][42][m],g[3][8],c
[42][42][2],f[42]; char d[42]; void v( int
b,int a,int j){ printf("\33[%d;%df\33[4%d"
"m  ",a,b,j); } void u(){ int T,e; n(42)o(
e,m)if(h[0][T][e]-h[1][T][e]){ v(e+4+e,T+2
,h[0][T][e]+12h[0][T][e]:0); h[1][T][e]=h[
0][T][e]; } fflush(stdout); } void q(int l
                ,int k,int p){
                int T,e,a; L=0
                ; O=1; while(O
                ){ n(4&&L){ e=
                k+c[l] [T][0];
                h[0][L-1+c[l][
                T][1]][p?20-e:
```

how to measure actual protections' effectiveness?

- **(self claimed) objective methods: software metrics**
  - are they good enough?
- **empirical analysis: experiments with people**
  - currently, the best approximation of the human brain is…
    - …the human brain

Empirical analysis: experiments involving people

- **subjects: experienced people that "approximate" software crackers / ethical hackers / penetration testers**
- **target: compromise assets in sample C applications / understand what functions written in C do**
- **objective: estimate the effectiveness of protection techniques with statistical methods**
- **this experiment?**
  - pre-hacking questionnaire
  - perform your hacking task
  - post-hacking questionnaire

What to do?

- ***register*, you will receive by email a link to a google form**
  - https://bit.ly/2Q2urax
- ***answer* a C programming questionnaire and *send* back answers (about 30 minutes)**
  - take your time but be fair
  - configure your programming environment
    - at least compile and debug
- ***experiment***
  - pre-questionnaire (about 10 minutes)
  - hacking experiment (about 3h)
    - try to crack programs/explain what you did in a post-questionnaire
- ***get***
  - up to 2/30 additional score (Sicurezza dei sistemi informatici)

When I get the 2 points?

- **receive the reward only for your availability and diligence**
  - honestly answer the C programming questionnaire
  - precisely answer the pre-hacking questionnaire
  - seriously try to crack the application
  - precisely and carefully answer the post questionnaire
    - where we ask you to (meticulously) report the activities you made when you tried to crack the application
      - by selecting a list of keywords from an ontology
    - …regardless of the fact that you succeeded or not
- **no dependence on successful cracking the app**
  - don't succeed but answer/report carefully → 2 points
  - succeed but too lazy to report very carefully → 0 (maybe 1)
  - just show up, minimum effort, and hope → 0 points

Bring your own PC

we cannot book labs big enough during the semester

- **1-2 rooms with electric sockets**

use your programming and hacking environment

- **any OS, will be standard C code**
- **software**
  - editor, compiler, IDE
  - debugger
  - software analysis tools
    - IDA pro (demo), radare2 (free), Ghidra (free)
      - decompilers / disassemblers not needed
      - but their plug-ins may
    - static code analysis, dynamic code analysis

Tentative dates and deadlines

- **register by November 18th**
- **send back the answers to the pre-experiment questionnaire by December 6th**
- **experiment**
  - December 14th
  - rooms to be communicated later

Some references and interesting readings

protections

- https://www.cs.auckland.ac.nz/~cthombor/Pubs/01027797a.pdf
- https://www.iacr.org/archive/crypto2001/21390001.pdf
- https://eprint.iacr.org/2013/083.pdf
- http://ieeexplore.ieee.org/document/4362895/
- https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2001-49.pdf

objective metrics

- http://link.springer.com/chapter/10.1007%2F3-540-44456-4_7

experiments

- http://selab.fbk.eu/ceccato/papers/2016/scam2016.pdf
- http://selab.fbk.eu/ceccato/papers/2014/emse2014a.html
- https://link.springer.com/article/10.1007%2Fs10664-019-09738-1

models

- https://arxiv.org/abs/1704.02774
- https://users.elis.ugent.be/~brdsutte/research/publications/2018EMSEceccato.pdf

the ASPIRE project

- https://aspire-fp7.eu/