Drošu sistēmu automātiska ģenerēšana no minimālas specifikācijas ...

Atis Straujums

2019. gada 27. februārī.

Zinātniskais vadītājs asoc. prof. Dr. Edgars Celms

Pietiekama sistēmas specifikācija

Sistēmām, kas paredzētas cilvēku lietošanai, eksistē vienkāršs apraksts. Šis apraksts ir viss, kas ir nepieciešams, lai atbilstošo sistēmu automātiski uzģenerētu.

Plāns

- Piemēri sistēmām, kurās intuitīvi ir nepieciešama drošība
- Kāpēc šīm sistēmām jābūt drošām?
- Kas īsti ir droša sistēma?
- Drošu sistēmu automātiska ģenerēšana
  - Sistēmas apraksta veidošana
  - Sistēmas ģenerēšana

Mērķi

- Rosināt pārdomas par to, ko nozīmē droša sistēma
- Ieskicēt sistēmu automātiskas ģenerēšanas sarežģītību

Kādām programmatūras sistēmām jābūt drošām, kāpēc?

- ?

Cerams, drošu programmatūras sistēmu piemēri

- Sociālais tīkls
- Mobilā lietotne banku maksājumiem
- Insulīna dozēšanas lietotne
- Gudrā māja
- Filmu straumēšanas serviss
- Automašīnas mezglu kontroles sistēma
- Dokumentu elektroniskā parakstīšana
- Ražošanas kontroles sistēma (SCADA)
- Dzelzceļa satiksmes kontroles sistēma
- Universitātes IT sistēma

Kāpēc šīm sistēmām jābūt drošām?

- Privātā dzīve, draugu loks, intereses, viedokļi, krāpšana, izmantojot svešu vārdu
- Finansiālais stāvoklis, maksājumu vēsture, nesankcionēti maksājumi
- Veselības stāvoklis, anamnēze, nepareiza lietošana ir bīstama veselībai
- Klātbūtnes noskaidrošana, izsekošana, nesankcionēta piekļuve īpašumam
- Pakalpojuma maksas apiešana, satura neatļauta pārpublicēšana
- Auto zādzība, kļūda sistēmā var novest pie avārijas
- Paraksta viltošana
- Atteice vai kļūda var radīt lielus materiālus zaudējumus
- Kļūda var novest pie katastrofas un dzīvību zaudēšanas
- Personīgie dati, izglītības informācija, izglītības dokumentu viltošana

Ko nozīmē “drošs”?

- Drošs: Tāds, kur nav jābīstas, neapdraudēts. Tāds, uz ko var paļauties.
  - Latviešu valodas vārdnīca, 1987
- Drošs = reliable; secure; tamper-proof; trustworthy; safe.
  Drošība = security; safety; safeguard; warrant; protection; surety
  - termini.lza.lv
- Secure: Fixed or fastened so as not to give way, become loose, or be lost; Certain to remain safe and unthreatened; Protected against attack or other criminal activity.
- Security: The state of being free from danger or threat;
- Safety: The condition of being protected from or unlikely to cause danger, risk, or injury.
  - en.oxforddictionaries.com

Droša sistēma (programmatūra, aparatūra, vide)

- Veic tai paredzētos darbus
  - Korekta
  - Uzticama
- Funkcionalitāti neietekmē nelabvēlīgi apstākļi
  - Komponenšu atteice ir paredzēta un tiek saprātīgi apstrādāta
- Nevar tikt izmantota nesankcionēti
  - Nav informācijas noplūdes
  - Resursi ir pieejami tikai paredzētiem lietotājiem
  - Ļaunprātīgi uzbrukumi tiek identificēti un atvairīti

Absolūti droša sistēma

Absolūti droša sistēma nodrošina tai paredzēto funkcionalitāti neatkarīgi no ārējo apstākļu iedarbības un nevar tikt izmantota nekādiem citiem mērķiem.

Absolūti drošu sistēmu nav

https://www.youtube.com/watch?v=pmbW0l1TxY4

Absolūti drošu sistēmu nav

- Eksistē funkcijas, kurām jebkura Tjūringa mašīna, kas rēķina kādu no šīm funkcijām, atklāj vairāk informācijas, nekā attiecīgās funkcijas orākuls (“melnā kaste”)
  - Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil P. Vadhan, Ke Yang. 2001. “On the (Im)possibility of Obfuscating Programs”
- Var definēt labāko iespējamo obfuskāciju kā funkciju, kas pārveido jebkuru Tjūringa mašīnu par tādu, kas atklāj ne vairāk informācijas, kā jebkura cita Tjūringa mašīna, kas rēķina to pašu funkciju
  - Shafi Goldwasser, Guy N. Rothblum. 2014. “On Best-Possible Obfuscation”
- Iespējams, līdzīgi var definēt arī maksimāli drošu sistēmu kā tādu, kas ir tik pat droša ka jebkura cita sistēma ar to pašu funkcionalitāti

Drošu sistēmu automātiska ģenerēšana

- Sistēmas apraksta veidošana
  - Funkcionalitātes apraksts
  - Pieejamo resursu / infrastruktūras izvēle
  - Risku pārvaldība
- Sistēmas ģenerēšana
  - Apraksta saprašana
  - Apdraudējumu veidi un aizsardzības iespējas
  - Implementācijas korektums

Sistēmas apraksta veidošana

- Aprakstu veido potenciālais lietotājs
- Funkcionalitātes apraksts (“Es gribu...”)
  - Es gribu pārskaitīt desmit eiro vecmāmiņai
  - Mēs ar kaimiņu gribam noskaidrot, kuram no mums ir vairāk naudas
- Drošības prasību apraksts (“Es negribu...”)
  - Es negribu, lai kāds var pārskaitīt naudu manā vietā, kā arī uzzināt cik un kam es pārskaitu
  - Mēs ar kaimiņu negribam atklāt otram, cik naudas mums ir
- Resursu norādīšana (“Man ir...”)
  - Man ir Android / Apple viedtālrunis ar Internet pieslēgumu
  - Mums ar kaimiņu katram ir papīrs ar zīmuli un kopīga sēta starp mums
- Risku pārvaldība (“Man vienalga / es pieņemu ...”)
  - Es pieņemu, ka kāds tomēr spēs pārskaitīt naudu manā vietā, ja viņam tam jāiztērē miljards eiro
  - Mums ar kaimiņu vienalga, ja kāds redzēs, ka mēs kaut ko kopīgi darām

Sistēmas apraksta veidošana

- Apgalvojums - drošības prasības nav jāspecificē, jo var pieņemt, ka lietotājs sākotnēji grib maksimāli drošu sistēmu
  - Vienkārši atskaldi nost visu, kas neizskatās pēc Dāvida! -Mikelandželo
    - Nav autentisks: https://quoteinvestigator.com/2014/06/22/chip-away/
- Praktisku apsvērumu dēļ lietotājam varētu nākties akceptēt kaut kādus riskus
  - Cena
  - Ātrdarbība
  - Pieejamie aizsardzības algoritmi / metodes
  - Pieejamie resursi (Android telefons ar standarta Internet pieslēgumu)

Apraksta saprašana

- Dabiskās valodas ir spēcīgas
  - noklusētas atsauces
  - kompresija
  - kontekstatkarība
- Kontekstatkarība pieprasa izpratni par jomu
  - Kodolfiziķim saprotams apraksts var nebūt saprotams citiem
- Aprakstos, ko veido cilvēki, ir kļūdas
  - Apraksta saprašana jāveic iteratīvi, jau apraksta veidošanas laikā

Kādi apdraudējumi pastāv šim sistēmām?

- Sociālais tīkls
- Mobilā lietotne banku maksājumiem
- Insulīna dozēšanas lietotne
- Gudrā māja
- Filmu straumēšanas serviss
- Automašīnas mezglu kontroles sistēma
- Dokumentu elektroniskā parakstīšana
- Ražošanas kontroles sistēma (SCADA)
- Dzelzceļa satiksmes kontroles sistēma
- Universitātes IT sistēma

Nepieciešami risinājumi visiem apdraudējumu veidiem

- Aparatūras atteice / infrastruktūras bojājums
- Pakalpojumatteices uzbrukums
- Pārtveršana / noklausīšanās (eavesdropping)
- Sociālā inženierija, pikšķerēšana
- Viltošana / mānīšana, izlikšanās (spoofing, impersonation)
- Privilēģiju eskalācija
- Tiešās piekļuves uzbrukumi
- “Sētas durvis” (backdoor)
- Manipulācijas uzbrukumi
- Blakusefektu uzbrukumi (side-channel attacks)

Implementācijas korektums

- Lai arī apraksts ir vienkāršs, sistēma var būt ļoti sarežģīta
- Ģenerēšanas rīks paļaujas uz solījumiem par izmantotajām komponentēm
- Komponenšu autoru uzdevums ir spēt pārliecināt par korektumu
  - Testēšana
  - Formālā verifikācija
- Komponentes deklaratīvā formā:
  - Ērtāka formālā verifikācija
  - Lielākas iespējas optimizēt / pielāgot rezultātu

Cilvēki par šo domā (jau kādu laiku!)

- IEEE Secure Development Conference
  - https://secdev.ieee.org/2019/papers/
- Dagstuhl Seminar,"Software Protection Decision Support and Evaluation Methodologies" (19331)
  - https://www.dagstuhl.de/de/programm/kalender/semhp/?semnr=19331
- Roman Knöll, Mira Mezini. 2006. “Pegasus: First Steps Toward a Naturalistic Programming Language”
  - https://dl.acm.org/citation.cfm?id=1176628
- LUMII Sistēmu modelēšanas un programmatūras tehnoloģiju laboratorija
- Un daudzi citi!

Turpmāko pētījumu virzieni

- Saistīti ar kriptogrāfiju
  - Ikdienas darbs SIA whiteCryption
- Specifikāciju apmierinošu kriptogrāfisku algoritmu un shēmu izvēle
  - Plaisa starp vajadzību pēc precīzas implementācijas un cilvēku zināšanām par kriptogrāfiju
- Jaunu kriptogrāfisku algoritmu un shēmu ģenerēšana konkrētam risinājumam
  - TLS? Kas ir TLS?

Paldies!

•••

atis.straujums@gmail.com