Universaalselt komponeeritavast ajatembeldusest

Peeter Laud

Tartu Ülikool ja Cybernetica AS

koostöös Ahto Buldase, Märt Saarepera ja Jan Willemsoniga

Ettekande plaan

- Mida tähendab süsteemi turvalisus?
- Milliste meetoditega seda näidata?
- Universaalne komponeeritavus.
- Ajatembeldus.
- Universaalselt komponeeritav ajatembeldus.

Funktsionaalsus ja turvalisus

- Funktsionaalsus — süsteem teeb midagi.
- Turvalisus — süsteem ei tee neid asju, mida me ei taha, et ta ei teeks.
  - Kõige turvalisem arvuti on väljalülitatud arvuti.
- Kaks sorti turvaomadusi:
  - Terviklus — Süsteemi võimalike jooksude seas ei ole halbu jookse.
  - Konfidentsiaalsus — Süsteemi kõik jooksud on mingis mõttes sarnased.
- Omaduste formalisatsioon on küllaltki keeruline.
  - Kasutatakse asümptootikuid.
    - Alternatiiv: loetakse täpselt arvutussamme.
  - Lubatakse kaduvväikest ebaõnnestumisvõimalust.

Süsteemide ülesehitus

- Süsteem koosneb komponentidest.
  - Mis koosnevad omakorda väiksematest komponentidest jne.
    - Lõpuks taandub kõik interaktiivsetele Turingi masinatele (ITM).
- Komponendid suhtlevad omavahel kasutades
  - läbi traadi või eetri vahetatud bitijadasid,
  - API väljakutseid,
  - jne.
- Süsteem ja ka komponendid võivad olla hajusad.
  - Aga iga ITM on ühes kindlas kohas.

Kuidas süsteemide üle arutleda?

- Süsteemide omadusi üritame tuletada tema komponentide omadustest.
  - Nii automaatselt kui võimalik.
    - programmide staatiline analüüs
    - mudelikontroll
    - teoreemide automaatne tõestamine
    - jne.
- Komponentide spetsifikatsioonid peaksid meile teada olema.
  - . . . ja olema antud kujul, mis hõlbustavad automatiseeritud arutelu.
    - „kompositsionaalsed“

Krüptograafilised primitiivid

- Krüptoprimitiivid on komponendid, mida kasutatakse turvaomaduste saavutamiseks.
- Näiteid:
  - sümmeetriline / asümmeetriline krüptimine;
  - digiallkirjad;
  - turvalised kanalid;
  - ajatembeldus;
  - e-valimised;
  - jne.
- Spetsifikatsioonid (turvadefinitsioonid) ütlevad, et teatud sorti käitumine pole võimalik.

Klassikalised turvadefinitsioonid

- . . . koosnesid
  - (formaliseeritud) stsenaariumite, mida vältida soovitakse, nimekirjast;
  - nõudest, et need kõigi mõistlike resurssidega ründajate jaoks kaduvväikese tõenäosusega toimuksid.
- Seega
  - krüptoprimitiivi kasutamine uuel viisil tähendab
  - uusi potentsiaalseid ohte tähendab
  - uusi definitsioone.
- Turvadefinitsioon — liikuv sihtmärk.

Arutletavus

- Turvadefinitsioon ei ütle midagi teiste stsenaariumite toimumise tõenäosuse kohta.
  - V.a. nende, mille võimalikkusest otseselt järeldub turvadefinitsioonis olevate stsenaariumite võimalikkus.
- Süsteemide üle neis terminites arutlemine ei ole lihtne.
  - Oleks vaja näidata, et suvaline süsteemis soovimatu stsenaarium sisaldab endas krüptoprimitiivi mõnda võimatut stsenaariumi.

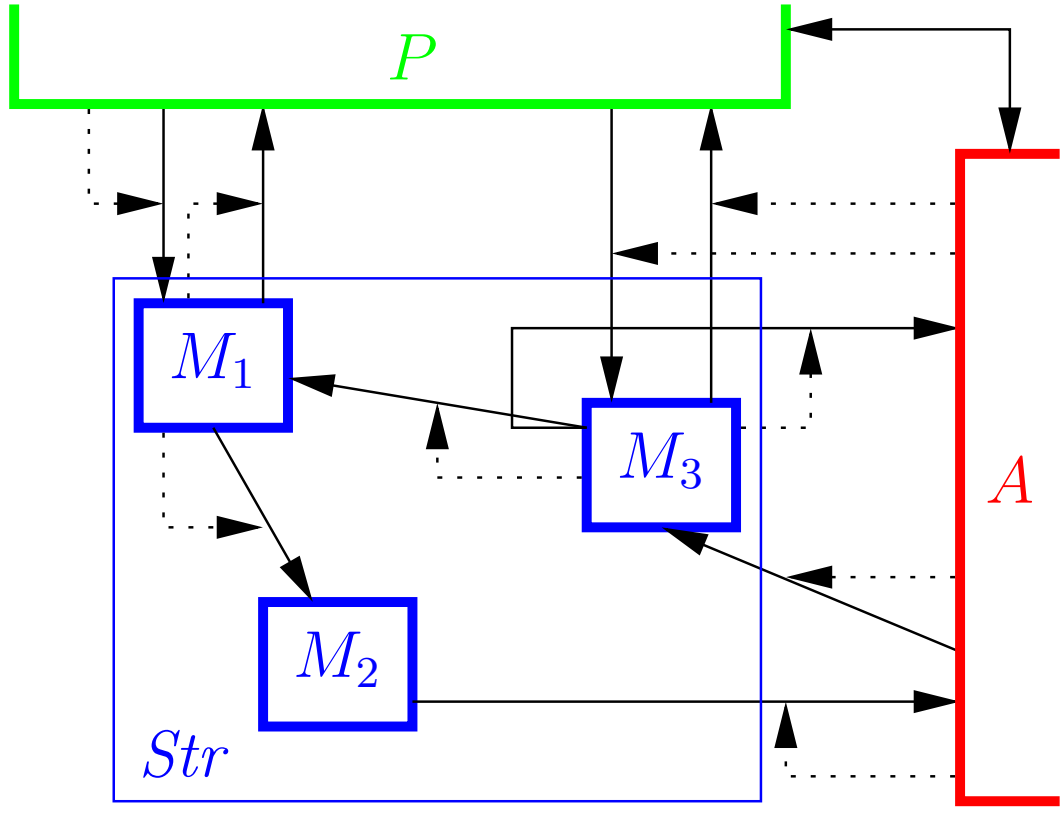
Def. realisatsioonide eristamatuse kaudu

- Nõuavad, et primitiiv oleks eristamatu mingist „ideaalsest primitiivist“.
- Ideaalne primitiiv on „ilmselt turvaline“.
- Näide: sümmeetrilise krüptimise ideaalne funktsionaalsus:
  - Initsialiseerimine: loo võti k.
  - x-i krüptimine: arvuta $y \leftarrow \mathcal{E}_k(\mathbf{0}^{|x|})$, salvesta (x, y), tagasta y.
  - y-i dekrüptimine — kui paar (x, y) on salvestatud, siis tagasta x, muidu tagasta $\mathcal{D}_k(y)$.
- Universaalne komponeeritavus — „eristamatus kõigis kontekstides“.

Primitiivide liidesed

- Süsteem on struktuuride hulk.
- Struktuur on ITM-ide kollektsioon.
- Masinate vahel on kanalid, kanalitel on nimed.
  - Masinatel on sisend- ja väljundpordid.
  - Kanalitel on puhvrid, kus teated edastamist ootavad.
  - Igal kanalil reguleerib edastamist mingi kindel masin.
- Vabad pordid — primitiivi liidesed. Kaks liidest:
  1. primitiivi kasutaja jaoks;
  2. ründaja jaoks.

Struktuur, masinad, kanalid, pordid



Reaalsed ja ideaalsed struktuurid

- Ideaalne struktuur on (tavaliselt) üksainus ITM.
  - Ta peaks meie arvates olema piisavalt turvaline.
  - . . . ja kontseptuaalselt lihtne.
    - Deterministlik.
    - Ründed võimatud, mitte kaduvväheselt tõenäolised.
- Reaalses struktuuris. . .
  - iga ITM on ühes kindlas kohas;
    - iga ITM-i ülesanne peaks olema nii väike kui võimalik.
  - turvalisi ja autentseid kanaleid tuleks kasutada vähe.

Näide halvast ideaalsest struktuurist

- Sümmeetrilise krüptimise ideaalne funktsionaalsus:
  - Initsialiseerimine: loo võti k.
  - x-i krüptimine: arvuta $y \leftarrow \mathcal{E}_k(\mathbf{0}^{|x|})$, salvesta (x, y), tagasta y.
  - y-i dekrüptimine — kui paar (x, y) on salvestatud, siis tagasta x, muidu tagasta $\mathcal{D}_k(y)$.
- Vajakajäämised:
  - krüptimine kasutab juhuarve;
  - sõltub reaalsest primitiivist;
  - võtit ei saa kastist kätte.

„realiseerib turvaliselt“

- Tahame, et reaalne struktuur realiseeriks ideaalse struktuuri turvaliselt.
- Struktuur Str realiseerib struktuuri Str' turvaliselt, kui

$$\forall P \forall A \exists A' : view_{P \| Str \| A}(P) \approx view_{P \| Str' \| A'}(P)$$

  tähistame $Str \geq Str'$.
- turvaline realiseerimine on ühtlane, kui

$$\forall A \exists A' \forall P : view_{P \| Str \| A}(P) \approx view_{P \| Str' \| A'}(P)$$

- turvaline realiseerimine on musta kasti meetodil, kui

$$\exists S \forall A \forall P : view_{P \| Str \| A}(P) \approx view_{P \| Str' \| (S \| A)}(P)$$

Mis on selles definitsioonis head?

- Kompositsiooniteoreem:

  Kui $Str_0 \geq Str_0'$ ja Str_1 on komponeeritav struktuuriga Str_0 või Str_0', siis $Str_1 \| Str_0 \geq Str_1 \| Str_0'$.

- "komponeeritav" — ei tohi ühenduda valede portide otsa.
  - Ründaja liides peab vabaks jääma.
  - Pordinimed peavad ühekordseks jääma.
- Kehtib ka ühtlase ja musta kasti meetodil realiseeritavuse jaoks.

Ajatembeldusfunktsionaalsus

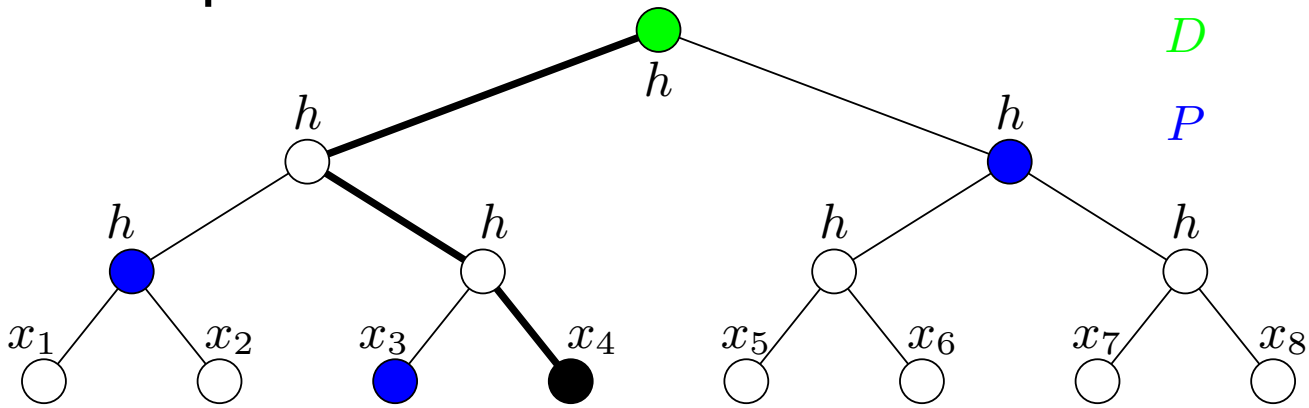
- Peaks defineerima järjestuse ajatembeldatud dokumentidel.
  - Kliendid esitavad dokumente ajatempliserverile (ATS).
  - ATS vastab ajatemplitega.
  - Kahe dokumendi ja neile võetud ajatemplite järgi peaks saama kindlaks teha nende ajatembeldamise järjekorra.
    - . . . vähemalt juhul, kui nende ajatembeldamiste vahe oli piisavalt pikk.
  - Uute ajatemplite lisamine olemasolevate ette peab olema võimatu.
- ATS ei ole usaldatud osapool.

Üks raundipõhine ajatempliskeem

- ATS kogub kokku kõik käesolevas raundis esitatud dokumendid.
- Peale raundi lõppu arvutab ta nende dokumentide akumuleeritud sõnumilühendi ja publitseerib selle.
  - „publitseerib“ = „tekitab ühisteadmuse“
- Ajatempel koosneb
  - raundinumbrist;
  - akumulatsiooni kuulumise tõestusest.
- Võrdlemine: antud kaks dokumenti ja nende ajatemplid:
  - võrdle raundinumbreid;
  - kontrolli akumulatsiooni kuulumise tõestusi publitseeitud sõnumilühendite suhtes.

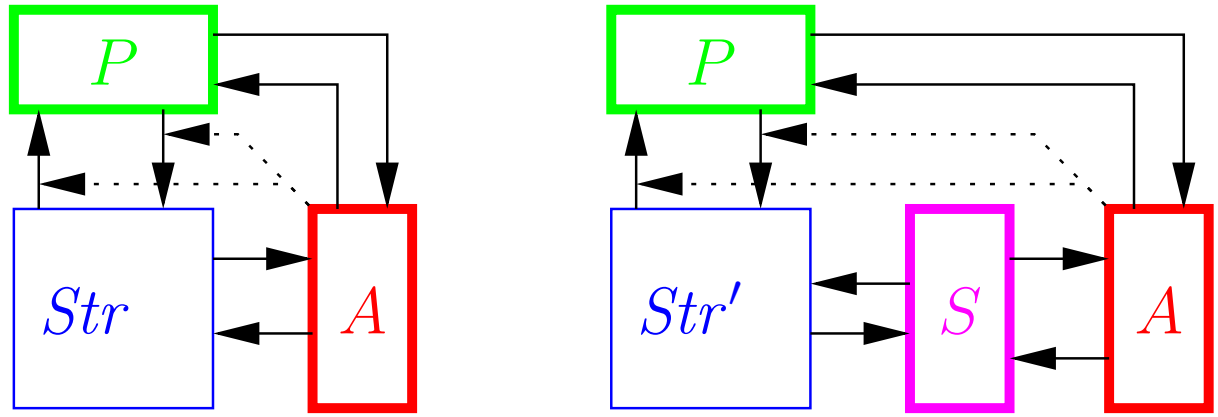
Akumulaatorid

- Akumulaator: funktsioon $D : \mathcal{P}_{\leq p(k)}(\{0,1\}^k) \to \{0,1\}^k$.
- Peale selle: kuulumistõestuse looja
  $P : \{0,1\}^k \times \mathcal{P}_{\leq p(k)}(\{0,1\}^k) \to \{0,1\}^*$
  ja kontrollija $V : \{0,1\}^k \times \{0,1\}^k \times \{0,1\}^* \to \mathbb{B}$.
- Kui $x \in X$, siis $V(x, D(X), P(x, X)) = \mathsf{true}$.
- Kui $x \notin X$, siis peab olema väga raske leida sellist p-d, et $V(x, D(X), p) = \mathsf{true}$.
- Näide: räsipuud.



Turvalise realiseerimise tõestamisest

- Tahame tõestada: $Str \geq Str'$ (musta kasti meetodil).
- Konstrueerime simulaatori S.
- Näitame, et $Str \cong (Str' \| S)$



- Selleks konstrueerime bisimulatsiooni struktuuride Str ja $Str' \| S$ olekute vahel.
  - Õigemini: vigadega bisimulatsiooni.
  - Näitame, et viga tekib kaduvväikese tõenäosusega.

Simulaatori konstrueerimisest

- Simulatoor tõlgib reaalse ja ideaalse maailma vahel.
- Mõnikord soovib ideaalne maailm andmeid, mis S-il reaalses maailmas veel käes ei ole.
  - Näide: S on saanud krüptoteksti ja soovib selle ideaalsele struktuurile Str' edastada.
  - Str' võib ka vastavat avateksti nõuda.
- S peab selle siis millegi eristamatuga asendama.
- See eristamatus peab ka süsteemi edasise töö käigus säiluma.
  - . . . olgugi et vahepeal rohkem infot saadakse.
- Kui ei saa asendada, siis ei ole ka simulaatorit.

Soovitud ideaalne funktsionaalsus $\mathcal{TS}_{\mathrm{id}}$

- Võta ajatemplipäringuid (stamp, x), edasta need ründajale.
- Kui ründaja vastab, siis edasta vastus kasutajale.
- Võta raundilõputeateid (EOR), edasta need ründajale.
- Võta ründajalt raundide sõnumilühendeid.
- Võta ründajalt ajatemplite kuulumistõestusi, edasta need ajatempli küsinud osapooltele.
- Võta kontrollimispäringuid $(\mathsf{verify}, x, c, \tau)$, kus
  - x on dokument;
  - c on kuulumistõestus;
  - τ on raundinumber

  ja vasta nendele.

Kontrollimispäringutele vastamine

- $\mathcal{TS}_{\mathrm{id}}$ võib ründajaga konsulteerida.
- Kui x ei eksisteerinud τ-nda raundi lõpus, siis ei tohi vastus olla yes.

Kontrollimispäringutele vastamine

- $\mathcal{TS}_{\mathrm{id}}$ võib ründajaga konsulteerida.
- Kui x ei eksisteerinud τ-nda raundi lõpus, siis ei tohi vastus olla yes.
- Mida tähendab „ei eksisteerinud“???

Kontrollimispäringutele vastamine

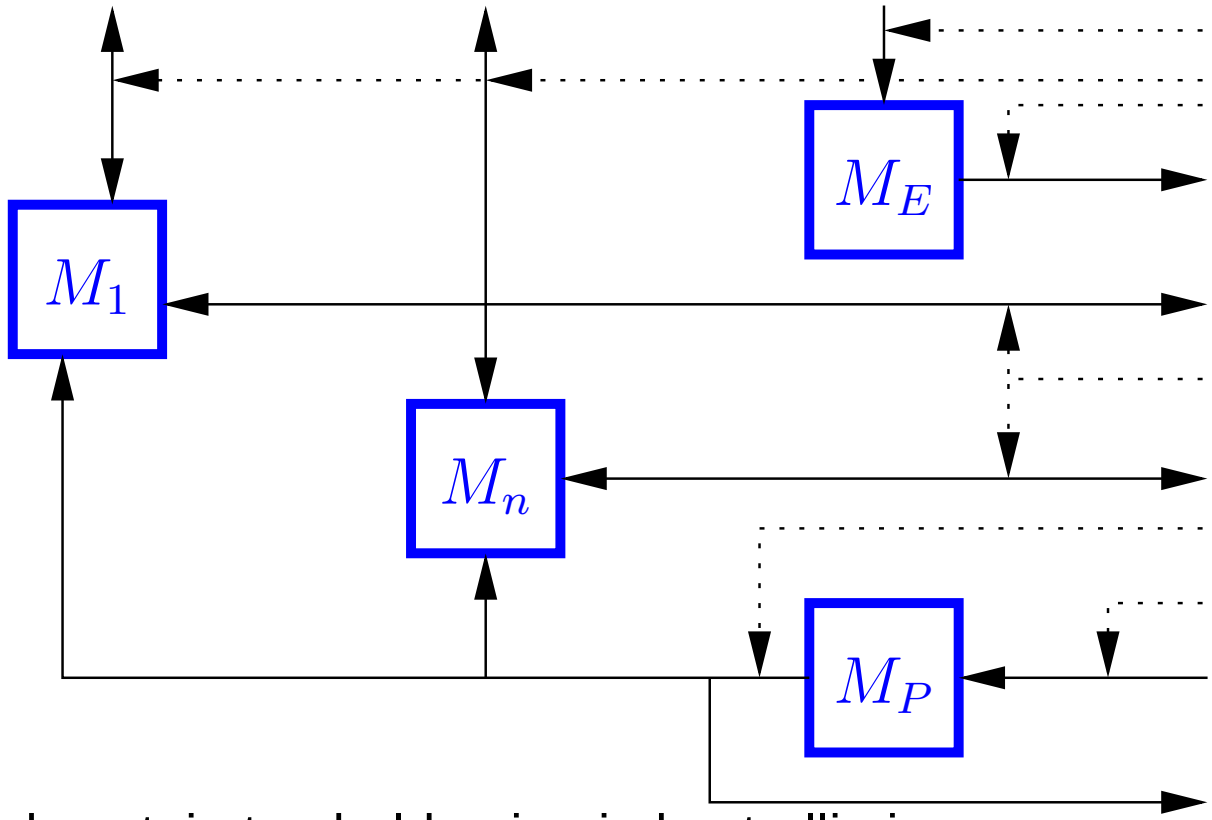
- $\mathcal{TS}_{\mathrm{id}}$ võib ründajaga konsulteerida.
- Kui x ei eksisteerinud τ-nda raundi lõpus, siis ei tohi vastus olla yes.
- Mida tähendab „ei eksisteerinud“???
- Võimalikud kompromissid:
  - Koos mingi raundi sõnumilühendiga annab ründaja kaasa ka kõigi selles raundis ajatembeldatud dokumentide nimekirja.
  - Loeme ajatembeldatuks ainult neid dokumente, millele küsiti ajatemplit funktsionaalsuse $\mathcal{TS}_{\mathrm{id}}$ kaudu.

Vastuste ajastamisest

- Reaalses struktuuris mingile päringule vastamisel on arvutuste tempo ründaja kontrolli all.
  - Vähemalt juhul, kui võrgus toimub liiklus.
- Kui ideaalne struktuur vastab sellele päringule viivitamatult, siis võib vastamiskiiruste erinevus märgatav olla.
- Ideaalne struktuur peab laskma ründajal endale öelda, millal päringutele vastata.

Koos mingi raundi sõnumilühendiga annab ründaja kaasa ka kõigi selles raundis ajatembeldatud dokumentide nimekirja.

Reaalne struktuur



M_i — i-nda kasutaja tembeldamine ja kontrollimine

M_E — raundilõputeated

M_P — saab ja publitseerib raundide sõnumilühendeid

Reaalne struktuur

- Masinad M_i
  - edastavad ajatembelduspäringuid ründajale
  - edastavad kuulumistõestuste päringuid ründajale ja tõestusi kasutajale tagasi;
  - saavad M_P-lt raundide sõnumilühendeid;
  - kontrollivad ajatempleid
    - . . . iseseisvalt.
- Masin M_E
  - edastab raundilõputeateid ründajale.
- Masin M_P
  - võtab vastu raundide sõnumilühendeid ja edastab need masinatele M_i.

Simulaator

- Simulaator peab kõigi ajatembeldatud dokumentide nimekirja ideaalsele funktsionaalsusele saatma.
  - Reaalne struktuur seda nimekirja ei saa.
  - Simulaator ei suuda sobivat listi konstrueerida. . .

Simulaator

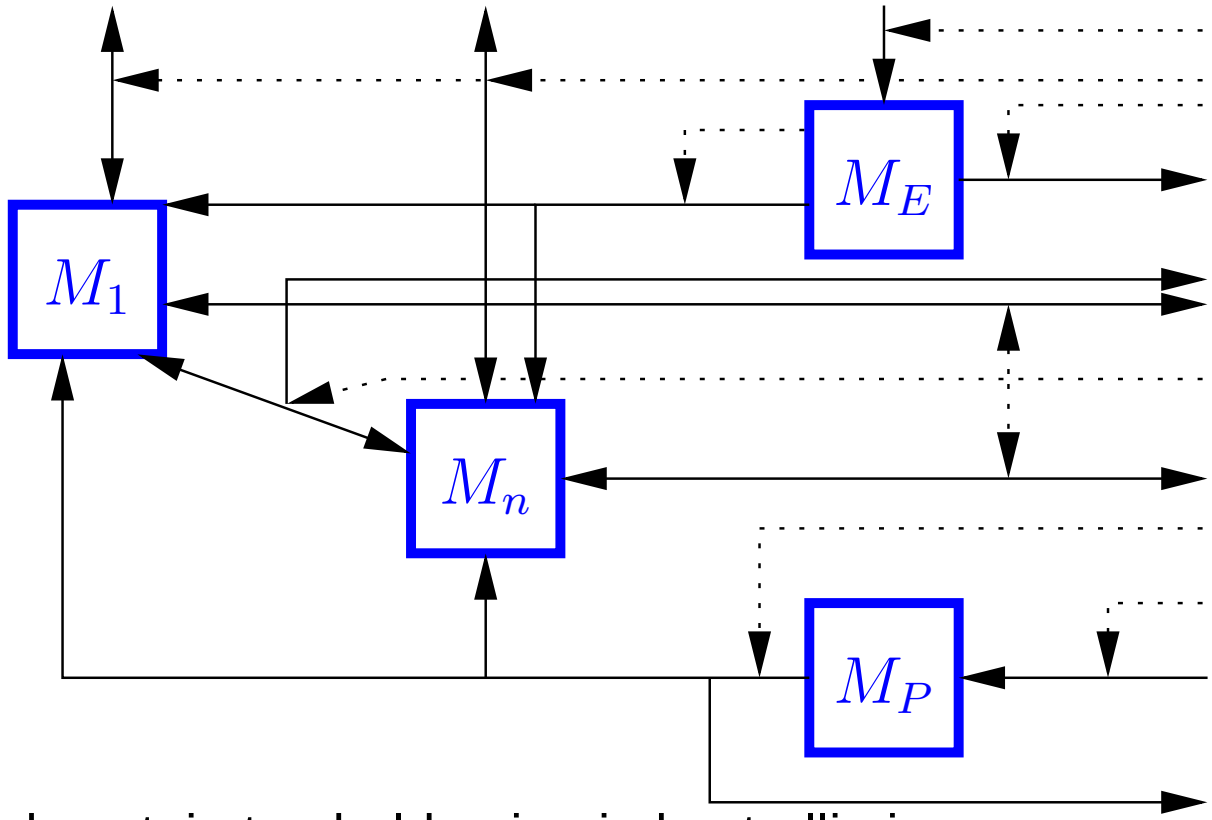
- Simulaator peab kõigi ajatembeldatud dokumentide nimekirja ideaalsele funktsionaalsusele saatma.
  - Reaalne struktuur seda nimekirja ei saa.
  - Simulaator ei suuda sobivat listi konstrueerida. . .
- Ründaja peab ka kõigi ajatembeldatud dokumentide nimekirja M_P-le saatma.
  - „auditeeritav ajatembeldus“
  - M_P peab sõnumilühendit selle nimekirja suhtes kontrollima.

Realisatsiooni head küljed

- Me suudame käsitleda sisse murtud osapooli.
  - Ründaja võib suvalise M_i oma kontrolli alla võtta.
    - Formalisatsioon: Saata $(\mathsf{corrupt})$ M_i-le.
    - Selle peale saadab M_i oma oleku ja edaspidi saadud teated ründajale ja saadab välja need teated, mis ründaja tal saata käsib.
  - Teiste poolte edaspidised ajatemplite kontrollimistulemused kehtivad edasi.
  - Ka ideaalne struktuur peab sisaldama sisse murtud osapoole mõistet.

Loeme ajatembeldatuks ainult neid dokumente, millele küsiti ajatemplit funktsionaalsuse $\mathcal{TS}_{\mathrm{id}}$ kaudu

Reaalne struktuur



M_i — i-nda kasutaja tembeldamine ja kontrollimine

M_E — raundilõputeated

M_P — saab ja publitseerib raundide sõnumilühendeid

Reaalne struktuur

- Masinad M_i
  - edastavad ajatembelduspäringuid ründajale
  - edastavad kuulumistõestuste päringuid ründajale ja tõestusi kasutajale tagasi;
  - saavad M_E-lt teateid raundide lõppemistest;
  - saavad M_P-lt raundide sõnumilühendeid;
  - kontrollivad, et ainult dokumendid, mis nad teatava raundi jooksul ajatembeldamiseks esitasid, kajastuvad sõnumilühendis (nende poolt ajatembeldatuna);
  - edastavad selle kontrolli tulemusi teistele M_j-dele;
  - kontrollivad ajatempleid;

Reaalne struktuur

- Masin M_E
  - edastab raundilõputeateid ründajale;
  - teavitab M_i-sid raundide lõppemisest.
- Masin M_P
  - Võtab vastu raundide sõnumilühendeid ja edastab need masinatele M_i.

Raundide sõnumilühendid

- Raundi nr. τ, sõnumilühend d_τ koosneb n-st sõnumilühendist $d_\tau^{(1)}, \ldots, d_\tau^{(n)}$.
- $d_\tau^{(i)}$ on kõigi i-nda kasutaja poolt τ-ndas raundis esitatud dokumentide sõnumilühend.
- M_i võib $d_\tau^{(i)}$ üle arvutada ja kontrollida, et ta ainult i-nda kasutaja poolt esitatud dokumente sisaldab.

Kokkuvõtvad märkused

- Me oleme konstrueerinud vajalikud simulaatorid ja bisimulatsioonid näitamaks, et need reaalsed struktuurid vastavaid ideaalseid struktuure turvaliselt realiseerivad.
- Universaalse komponeeritavuse raamvärk on osade krüptograafiliste primitiivide jaoks üpris raskesti kohaldatav.
- Kompromissid on vajalikud.
- Hea külg — kompositsiooniteoreem.