بسم الله الرحمن الرحیم

بهبود مکانیزم‌های مبتنی بر چنداجرایی برای اِعمال خط‌مشی‌های جریان اطلاعات

سید محمدمهدی احمدپناه

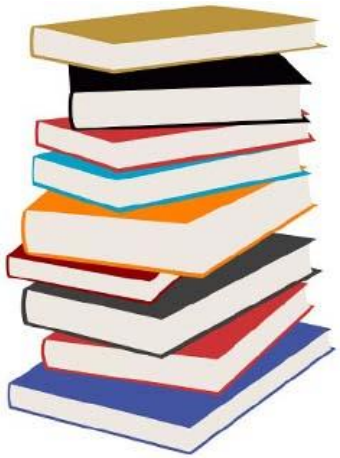
smahmadpanah@aut.ac.ir

استاد راهنما: دکتر مهران سلیمان‌فلاح

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

دانشگاه صنعتی امیرکبیر

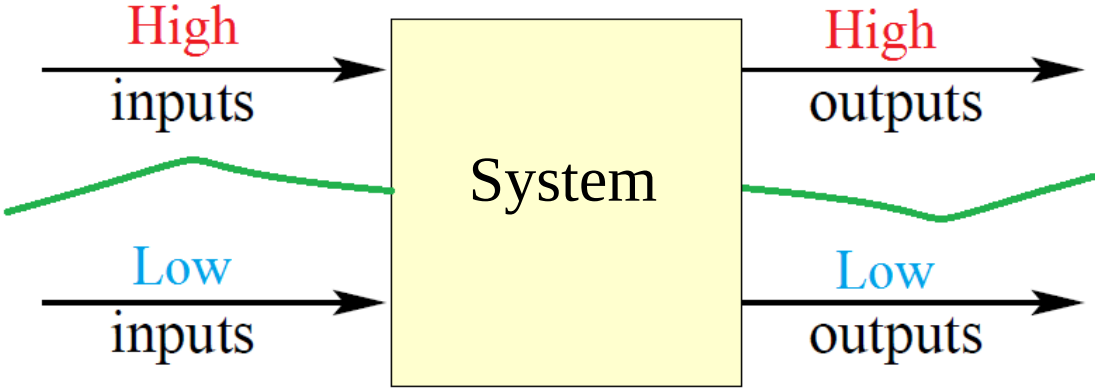
۲۹ مهر ۱۳۹۶



فهرست

- مقدمه و تعریف مسئله
  - خط‌مشی‌های جریان اطلاعات و عدم تداخل
  - انواع جریان‌های اطلاعات غیرمجاز
  - روش چنداجرایی امن
- مفاهیم اولیه
  - فوق خاصیت امنیتی
  - مکانیزم اعمال خط‌مشی‌های امنیتی
  - درستی و شفافیت
- دسته‌بندی کلی روش‌های اعمال خط‌مشی
- مقایسه مکانیزم‌های مبتنی بر چنداجرایی امن
- شرح مکانیزم پیشنهادی
- صوری‌سازی و اثبات
- جمع‌بندی و کارهای آینده

مقدمه



- تعری
  - مح
- تعری
- خط‌مشی امنیتی عدم تداخل
  - بیان گزاره‌هایی روی اجراهای برنامه
  - جریان اطا
    - جریان‌ها: ی به زمان

جریان اطلاعات غیرمجاز

- جریان صریح
- جریان ضمنی
- کانال نهان خاتمه
- کانال نهان زمانی
  - داخلی
  - خارجی

```
inH x;     // high input : x
if x = 0 then
    y = 1;
else
    skip;
outL y;    // low output : y
```

شکل ۱ – برنامه دارای جریان صریح

```
inH x;     // high input : x
if x = 0 then
    skip;
else
    skip;
outL y;    // low output : y
```

شکل۳ – برنامه دارای کانال نهان خاتمه

```
inH x;     // high input : x
if x = 0 then
    y = 1;
outL y;    // low output : y
```

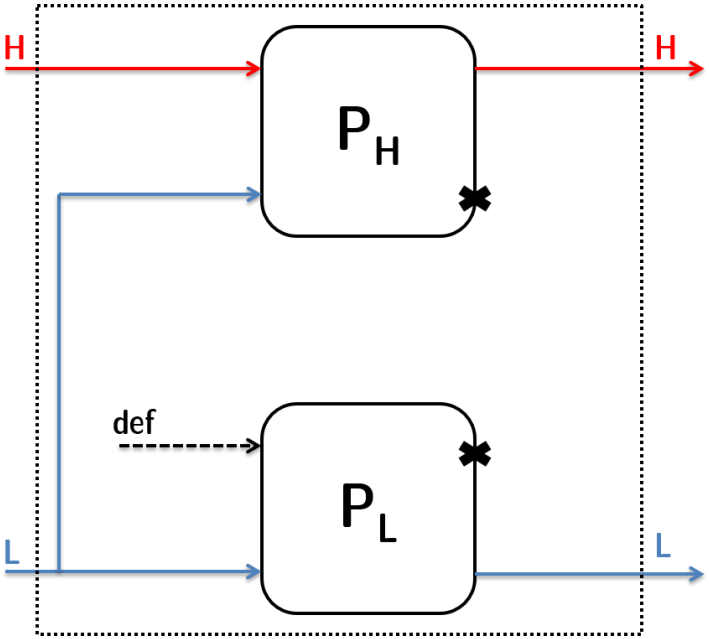
شکل۲ – برنامه دارای جریان ضمنی

```
if t > 2 then
    y = 1;
outL y;  // low output : y
```

شکل۴ – برنامه دارای کانال زمانی داخلی

روش چنداجرایی امن

- پویا و جعبه سیاه
- تهیه رونوشت از برنامه به تعداد سطوح امنیتی
- محدودیت روی ورودی‌ها و خروجی‌های هر رونوشت
- زمان‌بندی اجرای رونوشت‌ها



شکل۶ – نمایی از روش چنداجرایی امن [1]

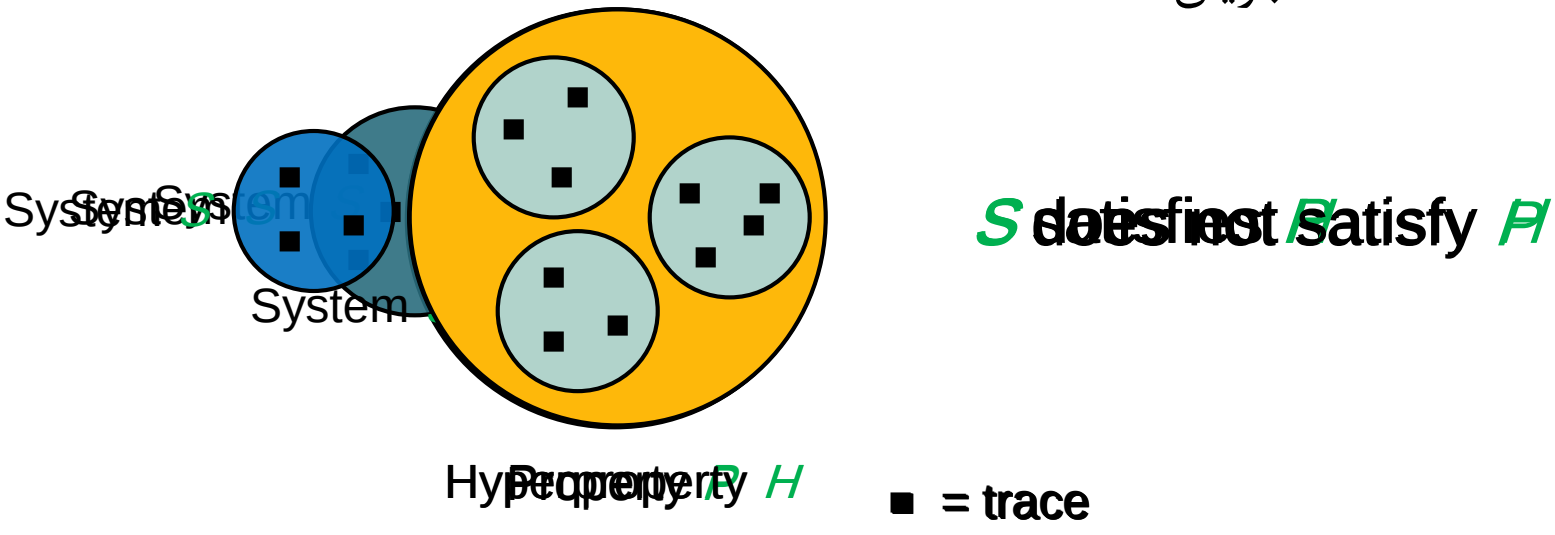
تعریف مسئله

- بهبود مکانیزم‌های مبتنی بر روش چنداجرایی امن
  - اعمال خط‌مشی عدم تداخل حساس به زمان
    - تضمین امنیت
    - حفظ ترتیب رویدادها در کانال‌های خروجی نسبت به یکدیگر برای اجراهای برنامه امن

- ایده کلی برای حل
  - استفاده از بافر و زمان‌بندی مناسب

خط‌مشی امنیتی؛ خاصیت‌ها و فوق‌خاصیت‌ها

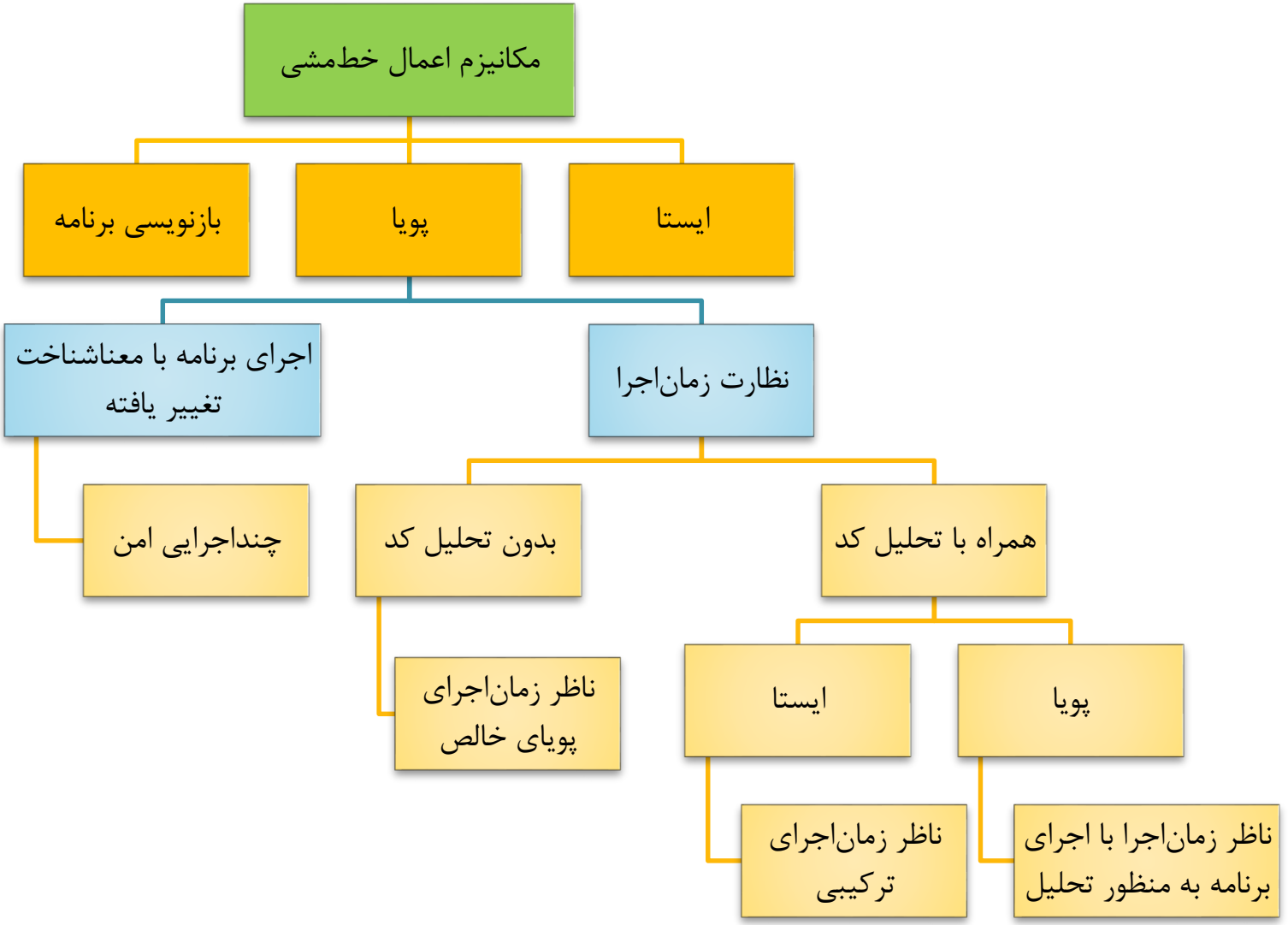
- خط‌مشی امنیتی
  - خاصیت: خط‌مشی‌های قابل تعریف روی تک اجرا
    - مانند کنترل دسترسی
  - فوق‌خاصیت: خط‌مشی‌های قابل تعریف روی مجموعه‌ای از اجراها [۲]
    - مانند جریان اطلاعات



مکانیزم اعمال خط‌مشی امنیتی

- مکانیزم اعمال امنیت
  - روش، ابزار یا رویه‌ای برای اعمال خط‌مشی امنیتی
- خواسته‌های مورد انتظار
  - درستی
    - همه برنامه‌ها پس از اعمال توسط مکانیزم امن باشند.
  - شفافیت
    - برنامه امن توسط مکانیزم نیز امن شناخته شود و دست نخورده بماند.

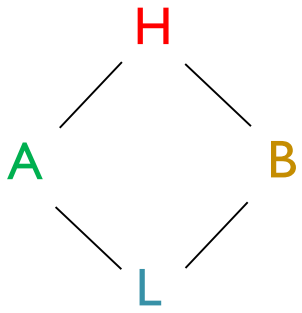
دسته‌بندی روش‌های اعمال خط‌مشی



شکل۸ – دسته‌بندی مکانیزم‌های اعمال خط‌مشی‌های امنیتی [۳]

مکانیزم‌های مبتنی بر چنداجرایی امن

- مکانیزم چنداجرایی امن با زمان‌بندی اولویت با سطح پایین‌تر [۱]
  - نقض امنیت برای سطوح غیرقابل مقایسه
  - امکان وقوع قحطی‌زدگی اجرای رونوشت‌های سطح بالا
  - حفظ ترتیب خروجی‌ها در هر کانال
- بررسی زمان‌بندهای مختلف و تأثیر آن‌ها در توانایی اعمال عدم تداخل [۴]
  - پیشنهاد زمان‌بندی *تسهیم* و مبتنی بر مشبکه

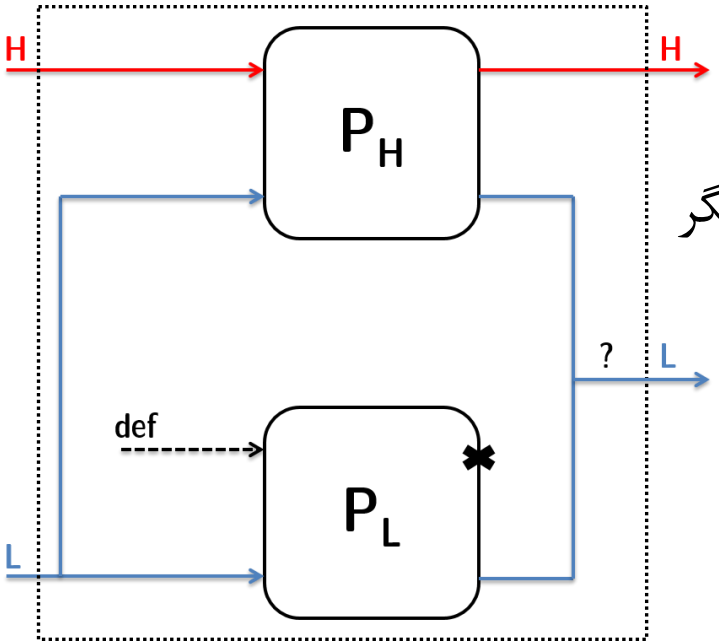


مکانیزم‌های مبتنی بر چنداجرایی امن (ادامه)

- بازنویس برنامه چنداجرایی امن [۵]
  - عدم تغییر محیط اجرا
- ناظر چنداجرایی امن [۶، ۷]
  - اجرای همزمان برنامه اصلی و چنداجرایی امن و مقایسه آن‌ها
  - حفظ ترتیب خروجی‌ها در هر کانال در اعمال حساس به خاتمه
  - پشتیبانی از کانال‌های پویا
  - عدم تضمین عدم تداخل حساس به زمان خارجی
- چنداجرایی امن نامتقارن [۸]
  - برش نامتقارن برنامه برای رونوشت سطح پایین

مکانیزم‌های مبتنی بر چنداجرایی امن (ادامه)

- Rafnsson و Sabelfeld[۹]
  - ایجاد تمایز بین سطح امنیتی حضور و محتوای پیام
  - پشتیبانی از خط‌مشی‌های حذف رده‌بندی
  - همگام‌سازی حصار
    - تضمین عدم تداخل حساس به خاتمه
    - حفظ ترتیب خروجی‌ها نسبت به یکدیگر



شکل۹ – چنداجرایی امن همراه با همگام‌سازی حصار [۹]

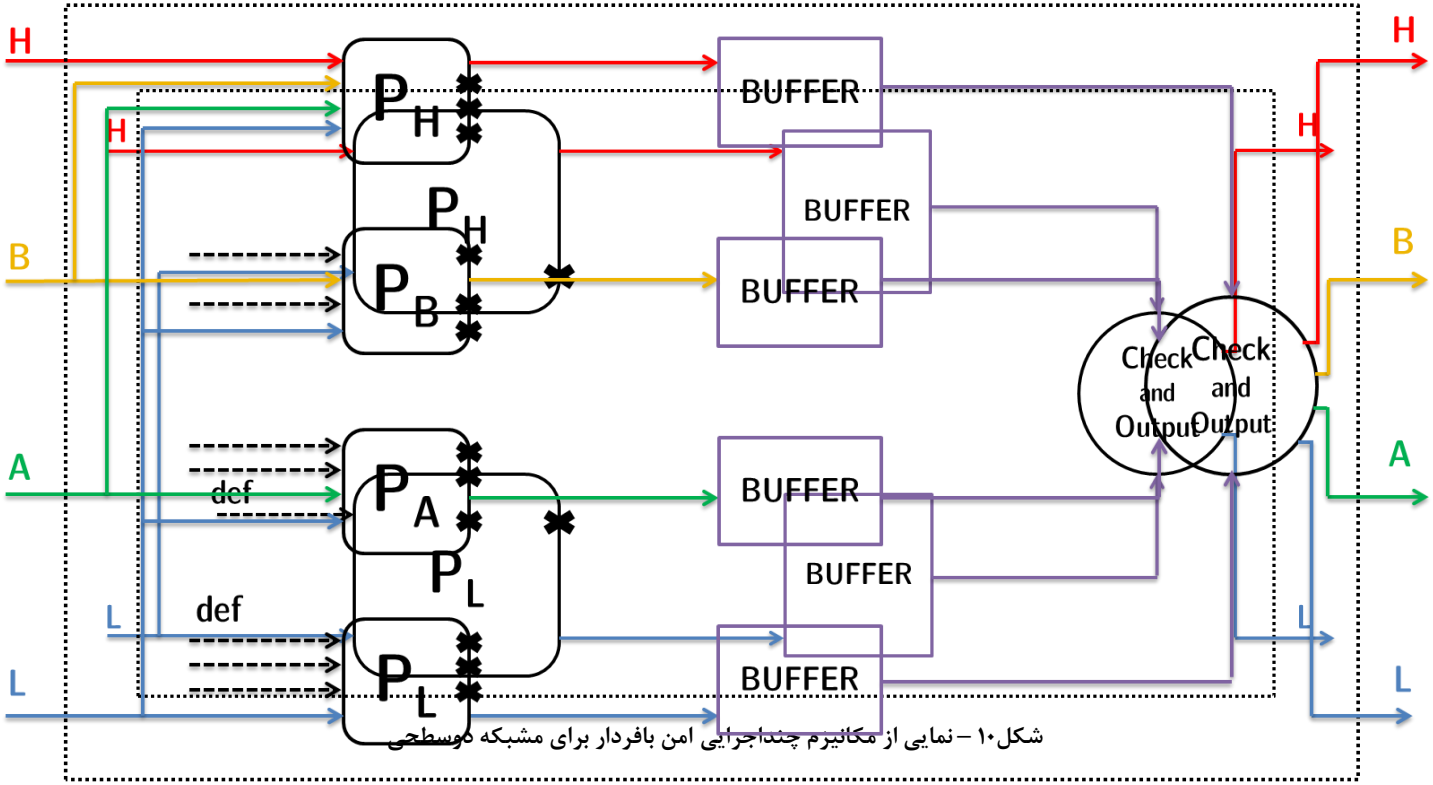
مروری بر مزایا و چالش‌های چنداجرایی امن

- امنیت به واسطه طراحی
- پویا و جعبه سیاه
  - مستقل از زبان برنامه‌نویسی و پیچیدگی‌های آن
- حفظ ترتیب رویدادهای خروجی در هر کانال به طور مستقل
- تغییر در ترتیب رویدادهای خروجی نسبت به یکدیگر
  - وابستگی به زمان‌بند
- عدم تشخیص نقض امنیت

**اعمال عدم تداخل حساس به زمان
همراه با حفظ ترتیب خروجی‌ها در کانال‌های مختلف
نسبت به یکدیگر**

شرح مکانیزم پیشنهادی

- چنداجرایی امن بافردار
- استفاده از زمان‌بندی تسهیم و اولویت با سطح پایین

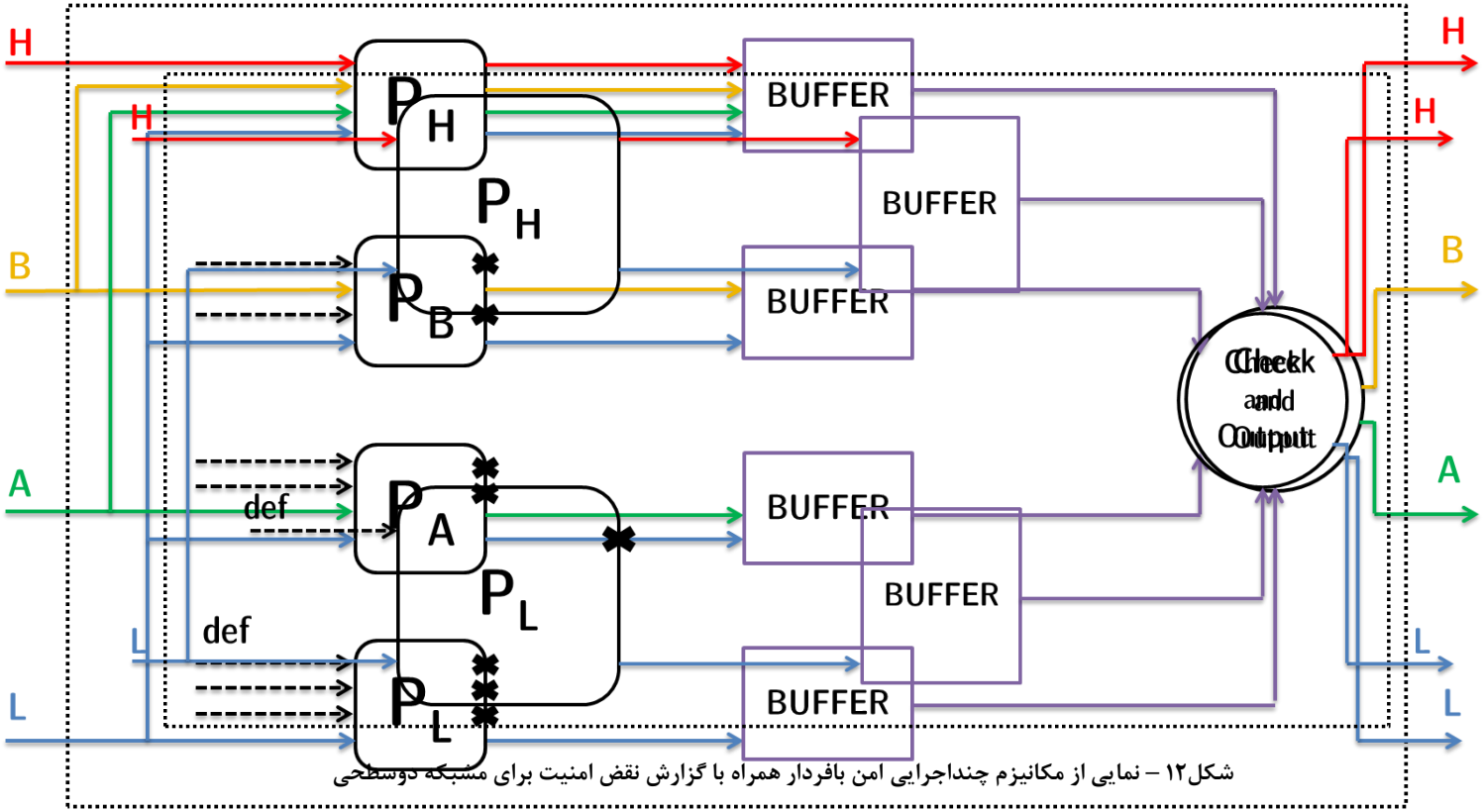


شکل۱۰ – نمایی از مکانیزم چنداجرایی امن بافردار برای مشبکه دوسطحی

شکل۱۱ – نمایی از مکانیزم چنداجرایی امن بافردار برای مشبکه چهارسطحی

شرح مکانیزم پیشنهادی (ادامه)

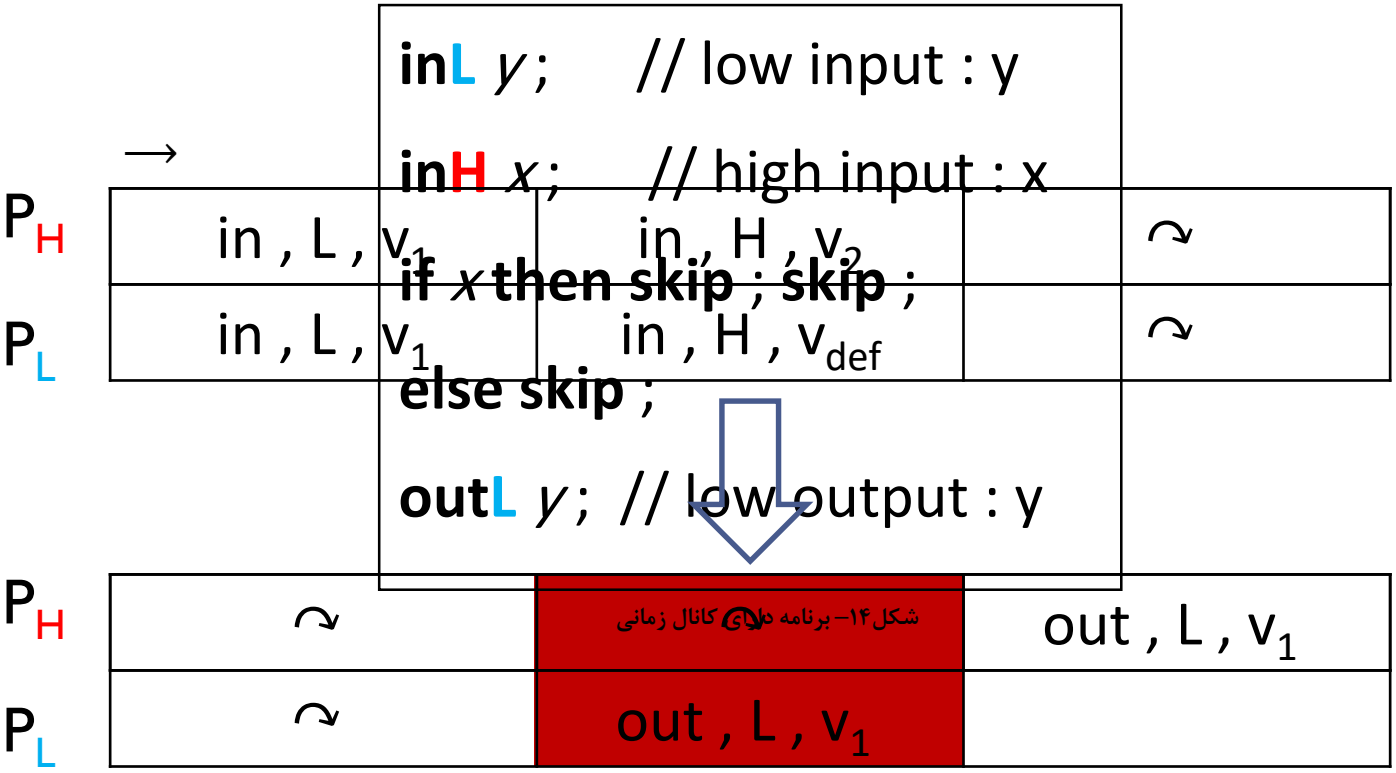
- حالت همراه با گزارش نقض امنیت



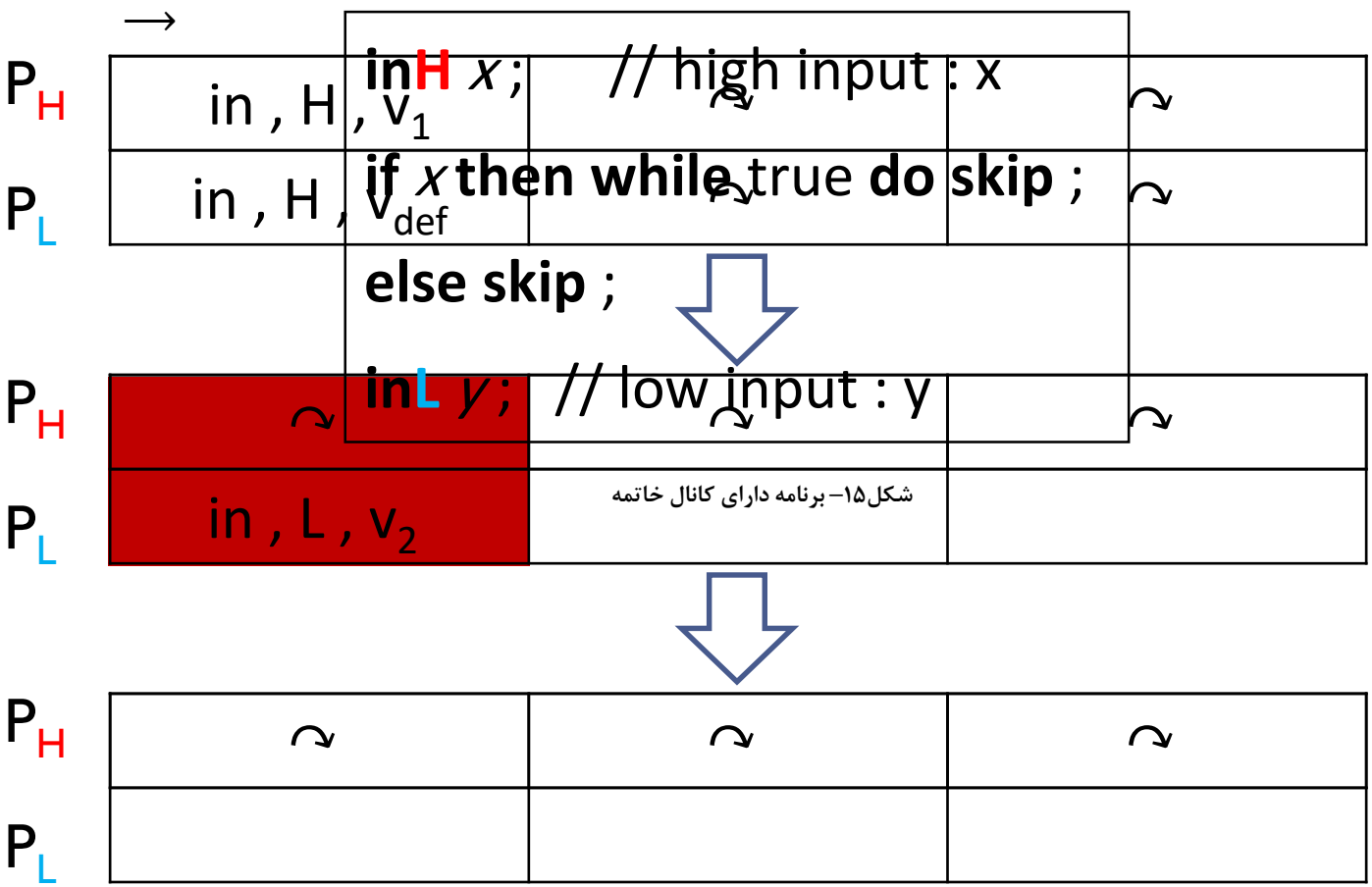
شکل۱۲ – نمایی از مکانیزم چنداجرایی امن بافردار همراه با گزارش نقض امنیت برای مشبکه دوسطحی

شکل۱۳– نمایی از مکانیزم چنداجرایی امن بافردار همراه با گزارش نقض امنیت برای مشبکه چهارسطحی

مثال‌هایی از نحوه اجرای مکانیزم پیشنهادی

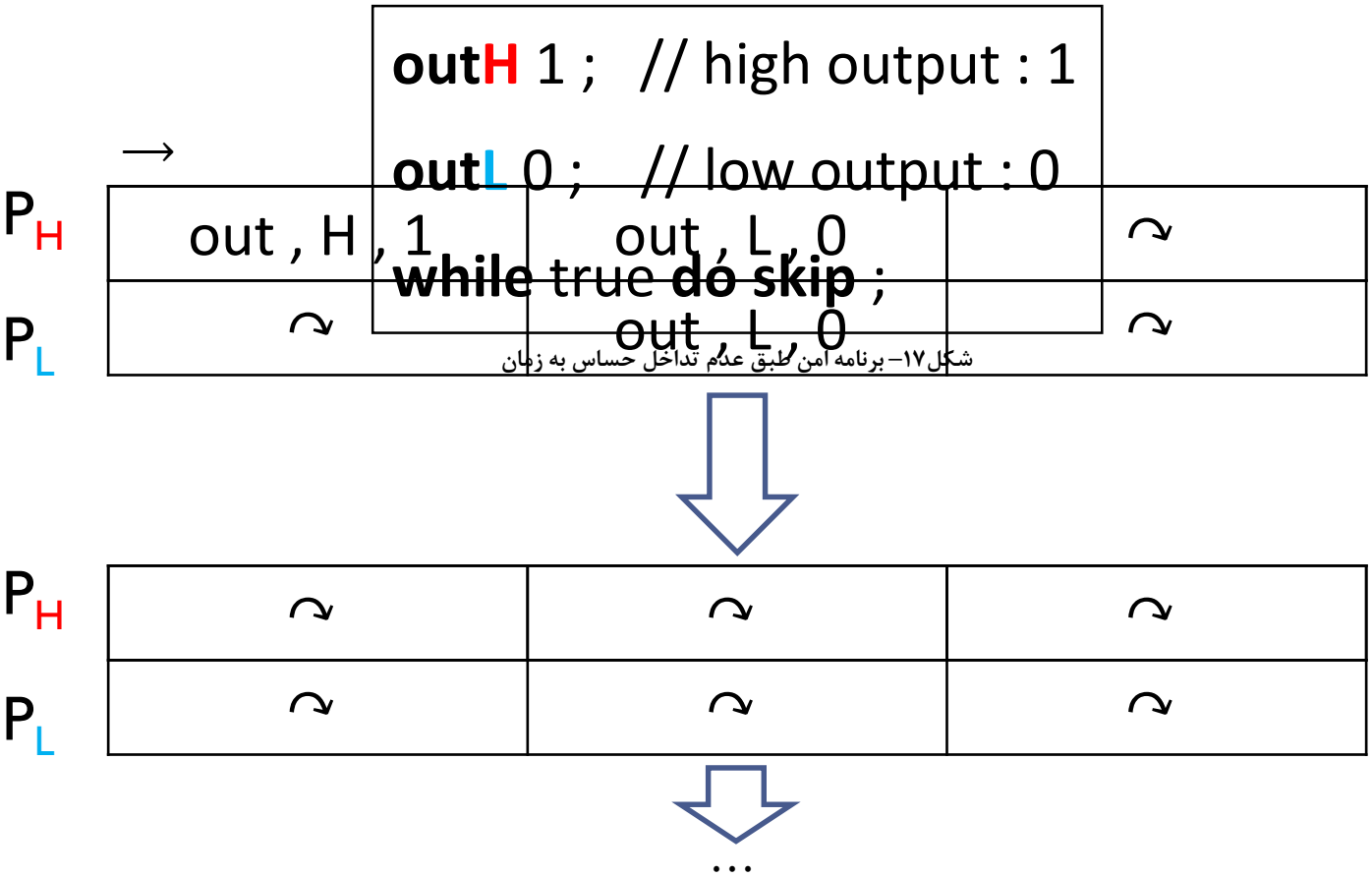


مثال‌هایی از نحوه اجرای مکانیزم پیشنهادی (ادامه)



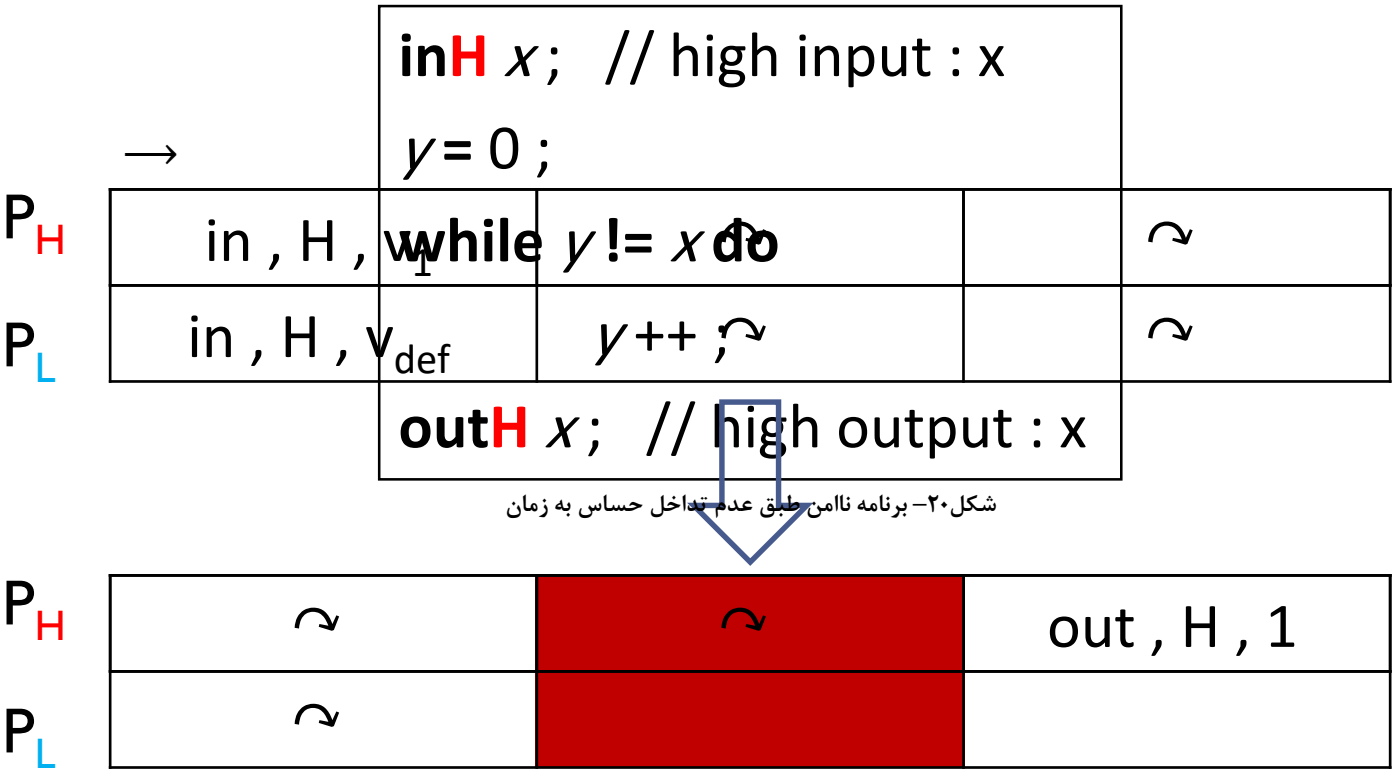
شکل۱۵– برنامه دارای کانال خاتمه

مثال‌هایی از نحوه اجرای مکانیزم پیشنهادی (ادامه)



شکل۱۷– برنامه امن طبق عدم تداخل حساس به زمان

مثال‌هایی از نحوه اجرای مکانیزم پیشنهادی (ادامه)



شکل۲۰– برنامه ناامن طبق عدم تداخل حساس به زمان

صوری‌سازی مکانیزم

- زبان مدل

$$
\begin{aligned}
c \;::=\;& x := e \\
\mid\;& c \;;\; c \\
\mid\;& \textbf{if } e \textbf{ then } c \textbf{ else } c \\
\mid\;& \textbf{while } e \textbf{ do } c \\
\mid\;& \textbf{skip} \\
\mid\;& \textbf{input } x \textbf{ from } i \\
\mid\;& \textbf{output } e \textbf{ to } o
\end{aligned}
$$

شکل ۲۱ – نحو دستورات موجود در زبان برنامه‌نویسی مدل

$$
\frac{I(i) = q \quad p(i) = n \quad q(n) = v}{read(I, i, p) = v}
$$

$$
\frac{O(o) = [v_1, \ldots, v_n]}{write(O, o, v) = O[o \mapsto [v_1, \ldots, v_n, v]]}
$$

صوری‌سازی مکانیزم (ادامه)

- پیکربندی اجرای استاندارد $\langle c,m,p,I,O \rangle$
- خاتمه

$$\langle P,m_0,p_0,I,O_0 \rangle \rightarrow^* \langle \mathbf{skip},m_f,p_f,I,O_f \rangle$$
$$(P,I) \rightarrow^* (p_f,O_f)$$

- رابطه اجرای زمان‌دار

$$\langle c,m,p,I,O \rangle \rightarrow^n \langle c',m',p',I,O' \rangle$$
$$(P,I) \rightarrow^n (p',O')$$

صوری‌سازی مکانیزم (ادامه)

$$\frac{c = \textbf{if } e \textbf{ then } c_{true} \textbf{ else } c_{false} \quad m(e) = b}{\langle c, m, p, I, O\rangle \rightarrow \langle c_b, m, p, I, O\rangle}$$

$$\frac{\langle c_1, m, p, I, O\rangle \rightarrow \langle {c'}_1, m', p', I, O'\rangle}{\langle c_1; c_2, m, p, I, O\rangle \rightarrow \langle {c'}_1; c_2, m', p', I, O'\rangle}$$

$$\frac{}{\langle \textbf{skip}; c, m, p, I, O\rangle \rightarrow \langle c, m, p, I, O\rangle}$$

$$\frac{c = \textbf{while } e \textbf{ do } c_{loop} \quad m(e) = true}{\langle c, m, p, I, O\rangle \rightarrow \langle c_{loop}; c, m, p, I, O\rangle}$$

$$\frac{c = \textbf{while } e \textbf{ do } c_{loop} \quad m(e) = false}{\langle c, m, p, I, O\rangle \rightarrow \langle \textbf{skip}, m, p, I, O\rangle}$$

$$\frac{m(e) = v \quad m' = m[x \mapsto v]}{\langle x := e, m, p, I, O\rangle \rightarrow \langle \textbf{skip}, m', p, I, O\rangle}$$

$$\frac{c = \textbf{output } e \textbf{ to } o \quad m(e) = v \quad O' = write(O, o, v)}{\langle c, m, p, I, O\rangle \rightarrow \langle \textbf{skip}, m, p, I, O'\rangle}$$

$$\frac{c = \textbf{input } x \textbf{ from } i \quad read(I, i, p) = v \quad p' = p[i \mapsto p(i) + 1] \quad m' = m[x \mapsto v]}{\langle c, m, p, I, O\rangle \rightarrow \langle \textbf{skip}, m', p', I, O\rangle}$$

شکل ۲۲ – معناشناخت کوته‌گام استاندارد زبان برنامه‌نویسی مدل [1]

صوری‌سازی مکانیزم (ادامه)

- معناشناخت محلی
  - نحوه اجرای رونوشت‌ها به طور مستقل از دیگری
  - پیکربندی محلی $\langle c,m,p,n\rangle_l$
- معناشناخت سراسری
  - همگام‌سازی و زمان‌بندی اجرای رونوشت‌ها
  - پیکربندی سراسری $\langle [lec_1, \dots, lec_j], r, I, O, B, s\rangle$

$$\langle L_0, r_0, I, O_0, B_0, s_0\rangle \mapsto^n \langle L_f, r_f, I, O_f, B_f, s_f\rangle$$

$$\frac{I(i) = q \quad p(i) = n \quad q(n) = v}{read(I, i, p) = v}$$

$$\frac{B(o) = [d_0, \dots, d_{t-1}] \quad 0 \le index < t}{write(B, o, d, index) = \mathrm{B(o)}[d_{index} \mapsto d]}$$

معناشناخت محلی

$$c = \textbf{output}\ e\ \textbf{to}\ o \quad m(e) = v \quad \sigma_{out}(o) = l$$

$$\frac{c = \textbf{if}\ e\ \textbf{then}\ c_{true}\ \textbf{else}\ c_{false} \quad m(e) = b \quad n' = n + 1}{\langle c, m, p, n\rangle_l, r, I, B \mapsto \langle c_b, m, p, n'\rangle_l, r, I, B}$$

$$\frac{\langle c_1, m, p, n\rangle_l, r, I, B \mapsto \langle c'_1, m', p', n'\rangle_l, r', I, B'}{\langle c_1; c_2, m, p, n\rangle_l, r, I, B \mapsto \langle c'_1; c_2, m', p', n'\rangle_l, r', I, B'}$$

$$\frac{c \qquad n' = n + 1 \qquad 1}{\langle \textbf{skip}; c, m, p, n\rangle_l, r, I, B \mapsto \langle c, m, p, n'\rangle_l, r, I, B}$$

$$\frac{c = \textbf{while}\ e\ \textbf{do}\ c_{loop} \quad m(e) = true \quad n' = n + 1}{\langle c, m, p, n\rangle_l, r, I, B \mapsto \langle c_{loop}; c, m, p, n'\rangle_l, r, I, B} \quad c = \quad \text{- 1]}$$

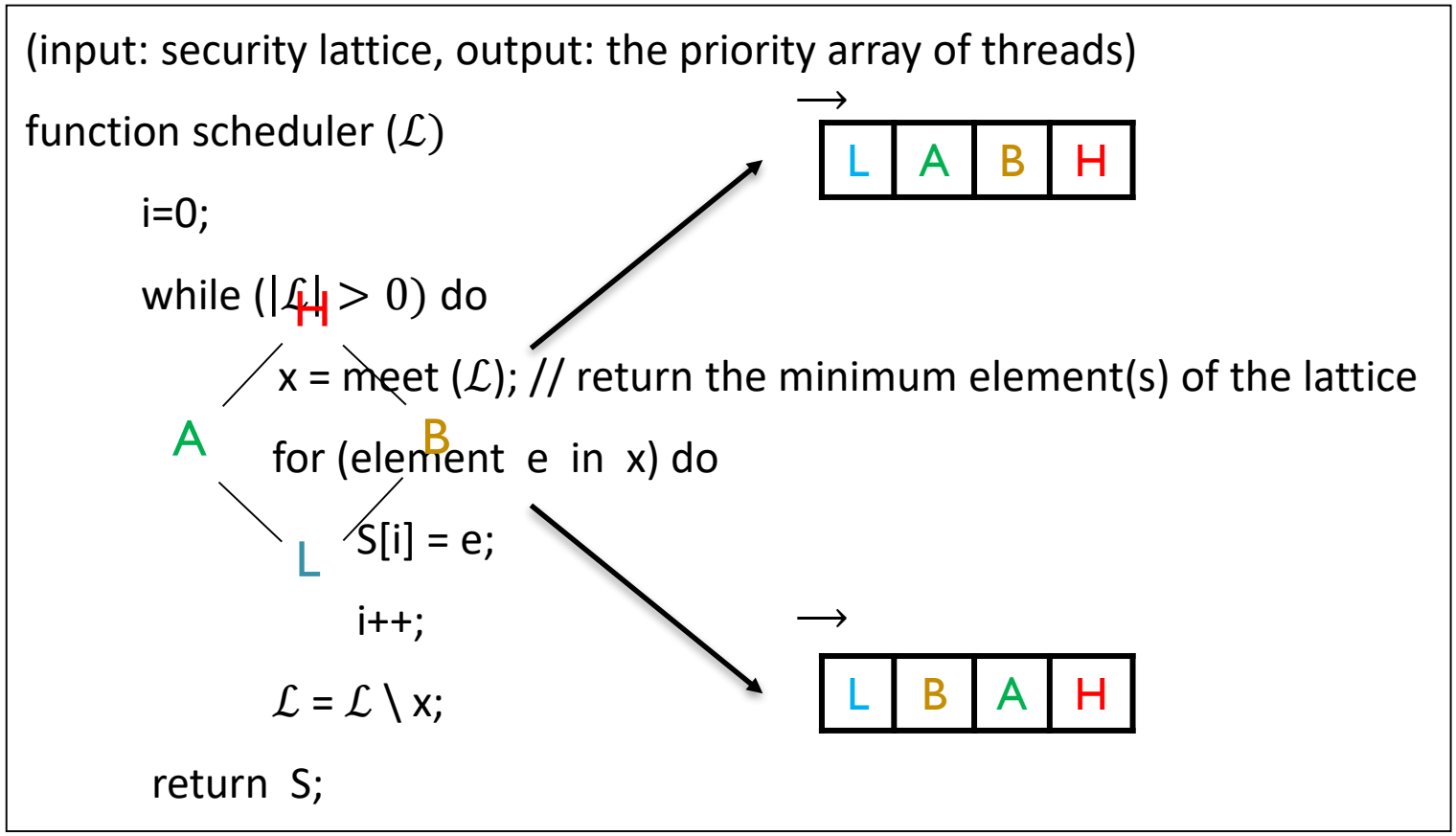
$$\frac{c = \textbf{while}\ e\ \textbf{do}\ c_{loop} \quad m(e) = false \quad n' = n + 1}{\langle c, m, p, n\rangle_l, r, I, B \mapsto \langle \textbf{skip}, m, p, n'\rangle_l, r, I, B}$$

$$\frac{m(e) = v \quad m' = m[x \mapsto v] \quad n' = n + 1}{\langle x := e, m, p, n\rangle_l, r, I, B \mapsto \langle \textbf{skip}, m', p, n'\rangle_l, r, I, B}$$

$$\langle c, m, p, n\rangle_l, r, I, B \mapsto \langle \textbf{skip}, m', p, n'\rangle_l, r, I, B$$

شکل ۲۲ – معناشناخت محلی چندمرحله‌ای امن بافردار بدون گزارش نقض امنیت

زمان‌بند مورد استفاده



شکل ۲۴ – تابع تعیین اولویت زمان‌بندی سطوح امنیتی

معناشناخت سراسری

- قسمت بررسی بافر و خروجی‌دادن

$$\frac{O(o_1) = [v_{11}, \dots, v_{1n}] \quad O(o_2) = [v_{21}, \dots, v_{2n'}] \quad \dots \quad O(o_s) = [v_{s1}, \dots, v_{sn''}]}{writeOut\left(O, (o_1, o_2, \dots, o_s), (v_1, v_2, \dots, v_s)\right) = O[o_1 \mapsto [v_{11}, \dots, v_{1n}, v_1], o_2 \mapsto [v_{21}, \dots, v_{2n'}, v_2], \dots, o_s \mapsto [v_{s1}, \dots, v_{sn''}, v_s]]}$$

$$\frac{k' = k + 1 \quad k \leq t - 1 \quad \forall o_s.\,(B(o_s)[k] = v \leftrightarrow (o_s, B(o_s)[k]) \in Temp) \quad O' = writeOut(O, Temp.o, Temp.v) \quad B' = B[\forall o_s.\,B(o_s)[k] \mapsto \emptyset]}{B, O, k \Mapsto B', O', k'}$$

$$\frac{k' = k + 1 \quad k \leq t - 1 \quad \forall o.\,B(o)[k] = \emptyset}{B, O, k \Mapsto B, O, k'}$$

شکل ۲۵ – معناشناخت قسمت بررسی و خروجی‌دادن در حالت عدم گزارش نقض امنیت

معناشناخت سراسری (ادامه)

$$\frac{s \neq j \quad lec = lec_s \quad s' = s + 1 \quad lec, r, I, B \Mapsto^t lec', r', I, B' \quad L' = L[lec \mapsto lec']}{\langle L, r, I, O, B, s \rangle \Mapsto^t \langle L', r', I, O, B', s' \rangle}$$

$$\frac{s = j \quad lec = lec_s \quad s' = 1 \quad lec, r, I, B \Mapsto^t lec', r', I, B' \quad L' = L[lec \mapsto lec'] \quad B', O, 0 \Mapsto^t B_0, O', t}{\langle L, r, I, O, B, s \rangle \Mapsto^{2t} \langle L', r', I, O', B_0, s' \rangle}$$

$$\frac{s = 1 \quad \forall lec_{index} \in L. lec_{index} = \langle \mathbf{skip}, m, p, n \rangle_l}{L = []}$$

شکل ۲۶ – معناشناخت سراسری برای چنداجرایی امن بافردار در حالت عدم گزارش نقض امنیت

اثبات درستی مکانیزم

- **تعریف ۱** (تعریف خط‌مشی عدم تداخل حساس به زمان) [۱] – برنامه P عدم تداخل حساس به زمان را طبق رابطه معناشناخت داده‌شده $\hookrightarrow^*$ برآورده می‌کند اگر برای هر سطح امنیتی $l \in \mathcal{L}$، برای هر $n \geq 0$، برای هر ورودی برنامه I و I' که $I =_l I'$ برای آن‌ها برقرار است، اگر $(p,O) \hookrightarrow^n (P,I)$، آنگاه $(p',O') \hookrightarrow^n (P,I')$، و $p =_l p'$ و $O =_l O$.

- **قضیه ۱** (درستی مکانیزم چنداجرایی امن بافردار) – هر برنامه P تحت مکانیزم چنداجرایی امن بافردار عدم تداخل حساس به زمان را برآورده می‌کند.

اثبات درستی مکانیزم (ادامه)

- **لم ۱** (نامتغیرهای حالت اجرای سراسری) – فرض کنید

$$\langle L_0, r_0, I, O_0, B_0, s_0\rangle \mapsto^n \langle L_f, r_f, I, O_f, B_f, s_f\rangle$$

پس خواهیم داشت،

- برای هر $\langle c,m,p,n\rangle_l \in L$، به ازای تمام $i \in C_{in}$ که $\sigma_{in}(i) = l$، $r(i)=p(i)$ است.
- برای هر سطح امنیتی l، فقط یک اجرا $\langle c,m,p,n\rangle_l$ در سطح امنیتی l در L وجود دارد.

- **لم ۲** (صیانت درستی برای معناشناخت محلی، بخش اول) – فرض کنید l_s یک سطح امنیتی و $l \leq l_s$ باشد. $\langle c,m,p,n\rangle_l, r_1, I_1, B_1 \mapsto \langle c',m',p',n'\rangle_l, r_1', I_1, B_1'$ را در نظر بگیرید و همچنین، فرض کنید $r_2 =_{l_s} r_1$، $I_2 =_{l_s} I_1$ و $B_2 =_{l_s} B_1$ برقرار باشد.

آنگاه $\langle c,m,p,n\rangle_l, r_2, I_2, B_2 \mapsto \langle c',m',p',n'\rangle_l, r_2', I_2, B_2'$ که در آن $r_2' =_{l_s} r_1'$ و $B_2' =_{l_s} B_1'$ است.

اثبات درستی مکانیزم (ادامه)

- **لم ۳** (صیانت درستی برای معناشناخت محلی، بخش دوم) – فرض کنید l_s یک سطح امنیتی و $l \not\leq l_s$ باشد. $\langle c,m,p,n\rangle_l,r,I,B \mapsto \langle c',m',p',n'\rangle_l,r',I,B'$ را در نظر بگیرید. بنابراین باید $r' =_{l_s} r$ و $B' =_{l_s} B$ باشد.

- **لم ۴** (صیانت درستی برای معناشناخت سراسری) – فرض کنید l_s یک سطح امنیتی باشد. در نظر بگیرید که

$$\langle L_1, r_1, I_1, O_1, B_1, s_1\rangle \mapsto \langle L_1', r_1', I_1, O_1', B_1', s_1'\rangle$$

و

$$\langle L_2, r_2, I_2, O_2, B_2, s_2\rangle \mapsto \langle L_2', r_2', I_2, O_2', B_2', s_2'\rangle$$

که $L_1 =_{l_s} L_2$، $r_1 =_{l_s} r_2$، $I_1 =_{l_s} I_2$، $O_1 =_{l_s} O_2$، $B_1 =_{l_s} B_2$ و $s_1 =_{l_s} s_2$ باشد. آنگاه به خاطر استفاده از زمان‌بند پیشنهادشده خواهیم داشت $L_1' =_{l_s} L_2'$، $r_1' =_{l_s} r_2'$، $O_1' =_{l_s} O_2'$، $B_1' =_{l_s} B_2'$ و $s_1' =_{l_s} s_2'$.

اثبات شفافیت کامل مکانیزم

- **قضیه ۲** (شفافیت کامل مکانیزم چنداجرایی امن بافردار) – اگر برنامه P عدم تداخل حساس به زمان را برآورده می‌کند، آنگاه برای هر ورودی برنامه I، برای هر $n \geq 0$، وجود دارد g و g' به طوری که

$$(P, I) \rightarrow^{n} (r_1, O_1) \Longrightarrow (P, I) \mapsto^{g} (r_1, O_1)$$

و

$$(P, I) \rightarrow^{n+1} (r_2, O_2) \Longrightarrow (P, I) \mapsto^{g'} (r_2, O_2)$$

که $g' > g \geq n$.

اثبات شفافیت کامل مکانیزم (ادامه)

- **لم ۵** (تناظر بین اجرای استاندارد و چنداجرایی امن بافردار) – فرض کنید $l \in \mathcal{L}$ و P یک برنامه باشد. در نظر بگیرید که

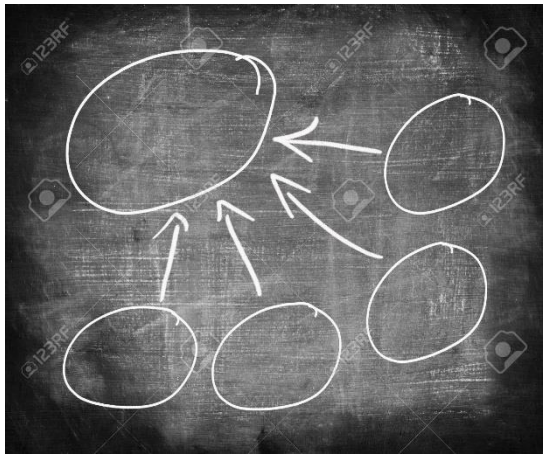
$$\langle L_{P,0}, r_0, I, O_0, B_0, s_0 \rangle \mapsto^{g} \langle L, r, I, O, B, s \rangle$$

که در آن $\langle c,m,p,n \rangle_l \in L$. تعریف می‌کنیم که $I_l = I_{|l}(i)$ است. آنگاه $\langle P, m_0, p_0, I_l, O_0 \rangle \rightarrow^{n} \langle c,m,p,I_l,O' \rangle$ خواهد بود که برای هر کانال خروجی o که $\sigma_{out}(o) = l$ باشد، $O'(o) = O(o)$ برقرار است. علاوه بر این، فرض کنید j تعداد سطوح امنیتی موجود در مشبکه و t مقدار سهم زمانی باشد. می‌دانیم که اندازه بافر هر سطح نیز برابر با t عنصر است. پس رابطه بین تعداد گام‌های محلی و سراسری اجرا تحت مکانیزم چنداجرایی امن بافردار و تعداد گام‌های اجرای استاندارد یک برنامه عبارت است از

$$g = (n/t).(j+1).t + j.t + n \bmod t$$

جمع‌بندی

- بهبود مکانیزم‌های مبتنی بر چنداجرایی امن برای اعمال خط‌مشی امنیتی عدم تداخل حساس به زمان و حفظ ترتیب رویدادهای خروجی نسبت به یکدیگر
  - مکانیزم چنداجرایی امن بافردار
- اثبات درستی و شفافیت کامل مکانیزم ارائه‌شده
- بررسی هزینه زمان اجرا



کارهای آینده

- پشتیبانی از حذف رده‌بندی
- کاهش سربار زمان اجرا
  - تکنیک‌های بهینه‌سازی
- پشتیبانی از قابلیت همروندی و عدم قطعیت
- انتخاب مقدار پیش‌فرض مناسب
- پیاده‌سازی مکانیزم پیشنهادی
- پیاده‌سازی چنداجرایی امن برای تلفن همراه

منابع و مراجع

[۱] D. Devriese and F. Piessens, "Noninterference through secure multi-execution," in *Proceedings - IEEE Symposium on Security and Privacy*, 2010, pp. 109–124.

[۲] M. R. Clarkson and F. B. Schneider, "Hyperproperties," *Journal of Computer Security*, vol. 18, no. 6, 2010, pp. 1157–1210.

[۳] A. Lamei, "Formal Characterization of Security Policy Enforcement through Program Rewriting," Ph.D. thesis, Amirkabir University of Technology, 2016..

[۴] V. Kashyap, B. Wiedermann, and B. Hardekopf, "Timing- and Termination-Sensitive Secure Information Flow: Exploring a New Approach," in *IEEE Symposium on Security and Privacy (S&P 2011)*, 2011, pp. 413–428.

[۵] G. Barthe, J. M. Crespo, D. Devriese, F. Piessens, and E. Rivas, "Secure multi-execution through static program transformation," in *Formal Techniques for Distributed Systems '12*, 2012, pp. 186–202.

[۶] D. Zanarini, M. Jaskelioff, and A. Russo, "Precise enforcement of confidentiality for reactive systems," in *Proceedings of the 2013 IEEE 26th Computer Security Foundations Symposium (CSF '13)*, 2013, pp. 18–32.

[۷] D. Zanarini and M. Jaskelioff, "Monitoring Reactive Systems with Dynamic Channels," in *Proceedings of the Ninth Workshop on Programming Languages and Analysis for Security*, 2014, pp. 66–78.

منابع و مراجع

[۸] I. Bolosteanu and D. Garg, "Asymmetric Secure Multi-execution with Declassification," in *Proceedings of the 5th International Conference on Principles of Security and Trust*, vol. 9635, Springer-Verlag New York, Inc., 2016, pp. 24–45

[۹] W. Rafnsson and A. Sabelfeld, "Secure Multi-execution: Fine-Grained, Declassification-Aware, and Transparent," in *2013 IEEE 26th Computer Security Foundations Symposium (CSF '13)*, 2013, pp. 33–48.

[۱۰] W. De Groef, D. Devriese, N. Nikiforakis, and F. Piessens, "Secure multi-execution of web scripts: Theory and practice," *Journal of Computer Security - Web Application Security*, vol. 22, no. 4, 2014, pp. 469–509.

[۱۱] M. Vanhoef, W. De Groef, D. Devriese, F. Piessens, and T. Rezk, "Stateful Declassification Policies for Event-Driven Programs," in *2014 IEEE 27th Computer Security Foundations Symposium (CSF '14)*, 2014, pp. 293–307.

[۱۲] M. Jaskelioff and A. Russo, "Secure multi-execution in haskell," in *Proceedings of the 8th International Conference on Perspectives of System Informatics*, 2012, pp. 170–178.

[۱۳] T. H. Austin and C. Flanagan, "Multiple facets for dynamic information flow," *ACM SIGPLAN-SIGACT Symposium on Principles of programming languages - POPL '12*, vol. 47, no. 1, 2012, p. 165-178.

منابع و مراجع

[۱۴] N. N. M. Ngo, "A Programmable Enforcement Framework for Security Policies," Ph.D. thesis, University of Trento, 2016.

[۱۵] N. Bielova and T. Rezk, "A taxonomy of information flow monitors," in *Proceedings of the 5th International Conference on Principles of Security and Trust*, vol. 9635, 2016, pp. 46–67.

[۱۶] N. Bielova and T. Rezk, "Spot the Difference: Secure Multi-execution and Multiple Facets," in *Computer Security – ESORICS 2016: 21st European Symposium on Research in Computer Security,* Springer International Publishing, 2016, pp. 501–519.

با سپاس از توجه شما! ☺