

# CIS 890: Language Based Security

Torben Amtoft & Anindya Banerjee  
Kansas State University

September 21, 2004

## Operational Semantics, part I

$$\text{(ASSIGN-OP)} \quad \frac{}{(x := e, \mu) \rightarrow (\text{nil}, \mu[\mu(e)/x])}$$

$$\text{(SEQ-OP1)} \quad \frac{(U, \mu) \rightarrow (U', \mu')}{(U; P, \mu) \rightarrow (U'; P, \mu')}$$

$$\text{(SEQ-OP2)} \quad \frac{(P, \mu) \rightarrow (P', \mu')}{(\text{nil}; P, \mu) \rightarrow (P', \mu')}$$

$$\text{(PAR-OP1)} \quad \frac{(P, \mu) \rightarrow (P', \mu')}{(P \parallel Q, \mu) \rightarrow (P' \parallel Q, \mu')}$$

$$\text{(PAR-OP2)} \quad \frac{(Q, \mu) \rightarrow (Q', \mu')}{(P \parallel Q, \mu) \rightarrow (P \parallel Q', \mu')}$$

## Operational Semantics, part II

$$\text{(COND-OP1)} \quad \frac{\mu(e) = tt}{(\text{if } e \text{ then } P \text{ else } Q, \mu) \rightarrow (P, \mu)}$$

$$\text{(COND-OP2)} \quad \frac{\mu(e) \neq tt}{(\text{if } e \text{ then } P \text{ else } Q, \mu) \rightarrow (Q, \mu)}$$

$$\text{(WHILE-OP1)} \quad \frac{\mu(e) = tt}{(\text{while } e \text{ do } U, \mu) \rightarrow (U; \text{while } e \text{ do } U, \mu)}$$

$$\text{(WHILE-OP2)} \quad \frac{\mu(e) \neq tt}{(\text{while } e \text{ do } U, \mu) \rightarrow (\text{nil}, \mu)}$$

## Typing Rules, part I

$$\text{(NIL)} \quad \frac{}{\Gamma \vdash \text{nil} : (\tau, \sigma) \text{ cmd}}$$

$$\text{(ASSIGN)} \quad \frac{\Gamma \vdash e : \tau, \Gamma(x) = \tau \text{ var}}{\Gamma \vdash x := e : (\tau, \sigma) \text{ cmd}}$$

$$\text{(PAR)} \quad \frac{\Gamma \vdash P_i : (\tau, \sigma) \text{ cmd}}{\Gamma \vdash P_0 \parallel P_1 : (\tau, \sigma) \text{ cmd}}$$

$$\text{(SUBTYPING)} \quad \frac{\Gamma \vdash P : (\tau, \sigma) \text{ cmd}, \tau' \leq \tau, \sigma \leq \sigma'}{\Gamma \vdash P : (\tau', \sigma') \text{ cmd}}$$

## Typing Rules, part II

$$(SEQ) \frac{\Gamma \vdash U : (\tau, \sigma) \text{ cmd}, \Gamma \vdash P : (\tau', \sigma') \text{ cmd}, \sigma \leq \tau'}{\Gamma \vdash U; P : (\tau \sqcap \tau', \sigma \sqcup \sigma') \text{ cmd}}$$

$$(COND) \frac{\Gamma \vdash e : \theta, \Gamma \vdash P_i : (\tau, \sigma) \text{ cmd}, \theta \leq \tau}{\Gamma \vdash \text{if } e \text{ then } P_0 \text{ else } P_1 : (\tau, \theta \sqcup \sigma) \text{ cmd}}$$

$$(WHILE) \frac{\Gamma \vdash e : \theta, \Gamma \vdash U : (\tau, \sigma) \text{ cmd}, \theta \sqcup \sigma \leq \tau}{\Gamma \vdash \text{while } e \text{ do } U : (\tau, \theta \sqcup \sigma) \text{ cmd}}$$

## Additional Operational Rules

$$\text{(WHEN-OP1)} \quad \frac{\mu(e) = tt, (U, \mu) \rightarrow (U', \mu')}{(\text{when } e \text{ do } U, \mu) \rightarrow (\text{when } e \text{ do } U', \mu')}$$

$$\text{(WHEN-OP2)} \quad \frac{\mu(e) = tt, (U, \mu) \not\rightarrow}{(\text{when } e \text{ do } U, \mu) \rightarrow (\text{when } e \text{ do } U, \mu)}$$

$$\text{(CONTROL-OP1)} \quad \frac{(P, \mu) \rightarrow (P', \mu'), (T, \mu) \rightarrow (T', \mu'')}{(P[T], \mu) \rightarrow (P'[T'], \mu' \sqcup_{\mu} \mu'')}$$

$$\text{(CONTROL-OP2)} \quad \frac{(P, \mu) \rightarrow (P', \mu'), (T, \mu) \not\rightarrow}{(P[T], \mu) \rightarrow (P'[T], \mu')}$$

## Additional Typing Rules

$$\text{(WHEN)} \quad \frac{\Gamma \vdash e : \theta, \Gamma \vdash U : (\tau, \sigma) \text{ cmd}, \theta \leq \tau}{\Gamma \vdash \text{when } e \text{ do } U : (\tau, \theta) \text{ cmd}}$$

$$\text{(CONTROL)} \quad \frac{\Gamma \vdash P : (\tau, \sigma) \text{ cmd}, \Gamma \vdash T : (\tau, \sigma) \text{ cmd}, \sigma \leq \tau}{\Gamma \vdash P[T] : (\tau, \sigma) \text{ cmd}}$$