

Hyperproperties



Florian Guthmann, 2026-07-09

Systems can be correct yet insecure

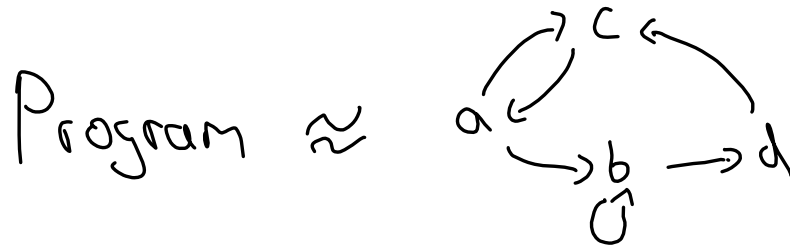
Correctness

"Every computation produces correct results"

Security

"An attacker cannot distinguish computations with different secrets"

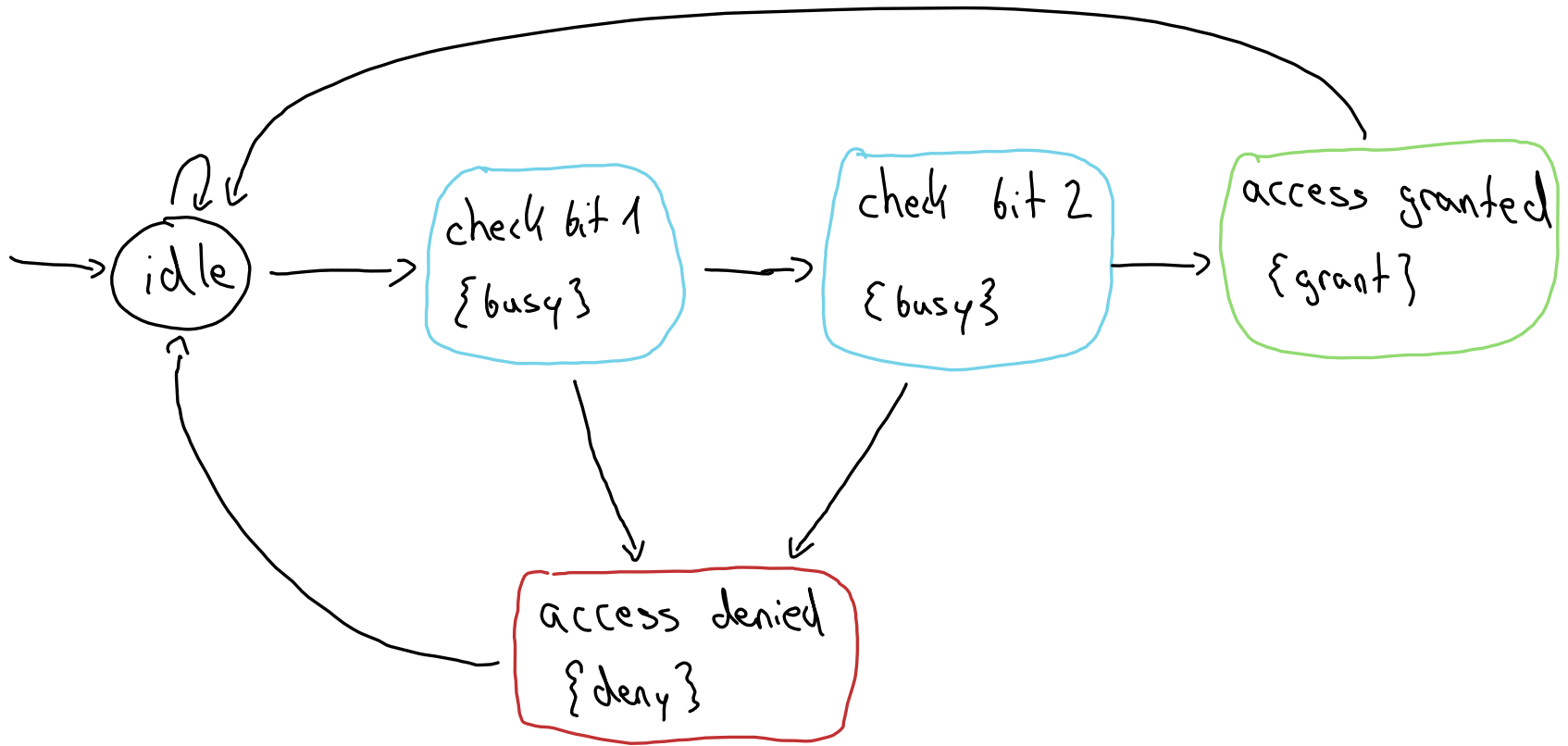
Verifying Correctness



Execution $\approx a \rightarrow b \rightarrow b \rightarrow d \rightarrow \dots$

Correctness Property $\approx$ Property of a single execution

2-Bit Password Checker



• high inputs: $secret_1, secret_2$

• outputs: $busy, deny, grant$

• low inputs: $guess_1, guess_2$

Linear Time Logic *

Correctness Property = LTL - formula

* Pnueli, 1977

Propositional Connectives

$\perp \Leftrightarrow$ "never holds"

$\top \Leftrightarrow$ "always holds"

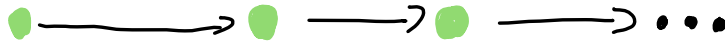
$\varphi \wedge \psi \Leftrightarrow$ " φ holds and ψ holds"

$\varphi \vee \psi \Leftrightarrow$ " φ holds or* ψ holds"

$\varphi \Rightarrow \psi \Leftrightarrow$ "if φ holds, then ψ holds"

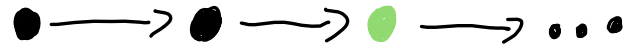
* inclusive or

Globally



$G \varphi \Leftrightarrow$ "It is always the case that φ holds"

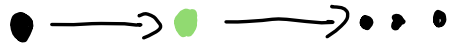
Finally



$\text{F } \varphi \Leftrightarrow$ "at some point in the future, φ holds"



ne X_t



$X \varphi \Leftrightarrow$ "in the next step, φ holds"

Until



$\varphi \text{ U } \psi \Leftrightarrow$ "at some point in the future, ψ holds
and φ holds at all times before that"

Correctness of the 2-Bit Password Checker

- Mutual exclusion

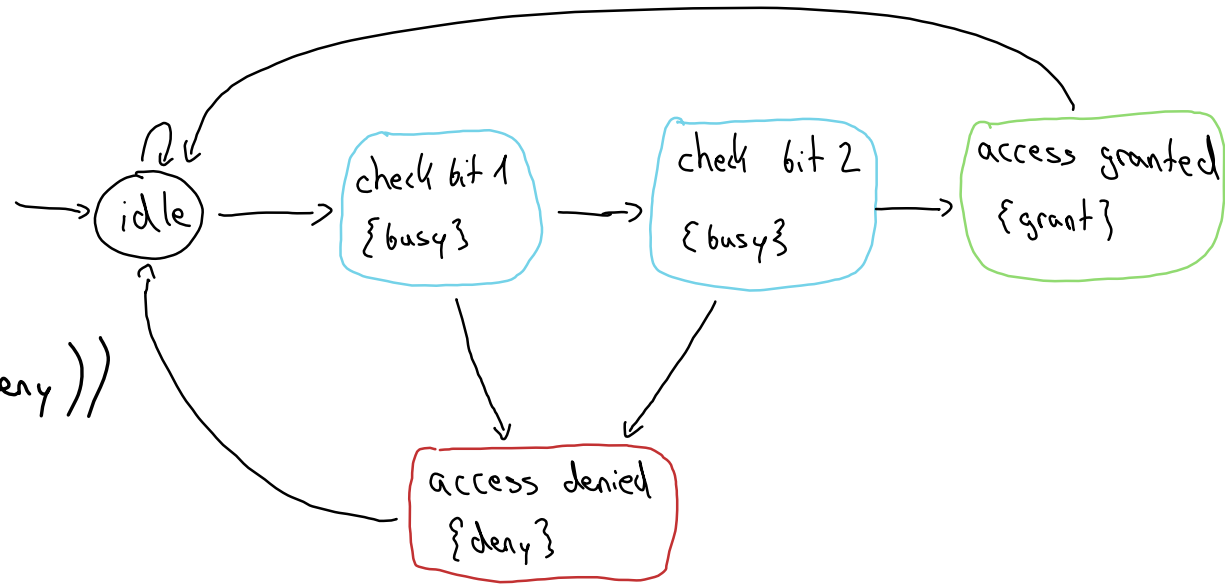
$G \neg (\text{grant} \wedge \text{deny})$

- Liveness

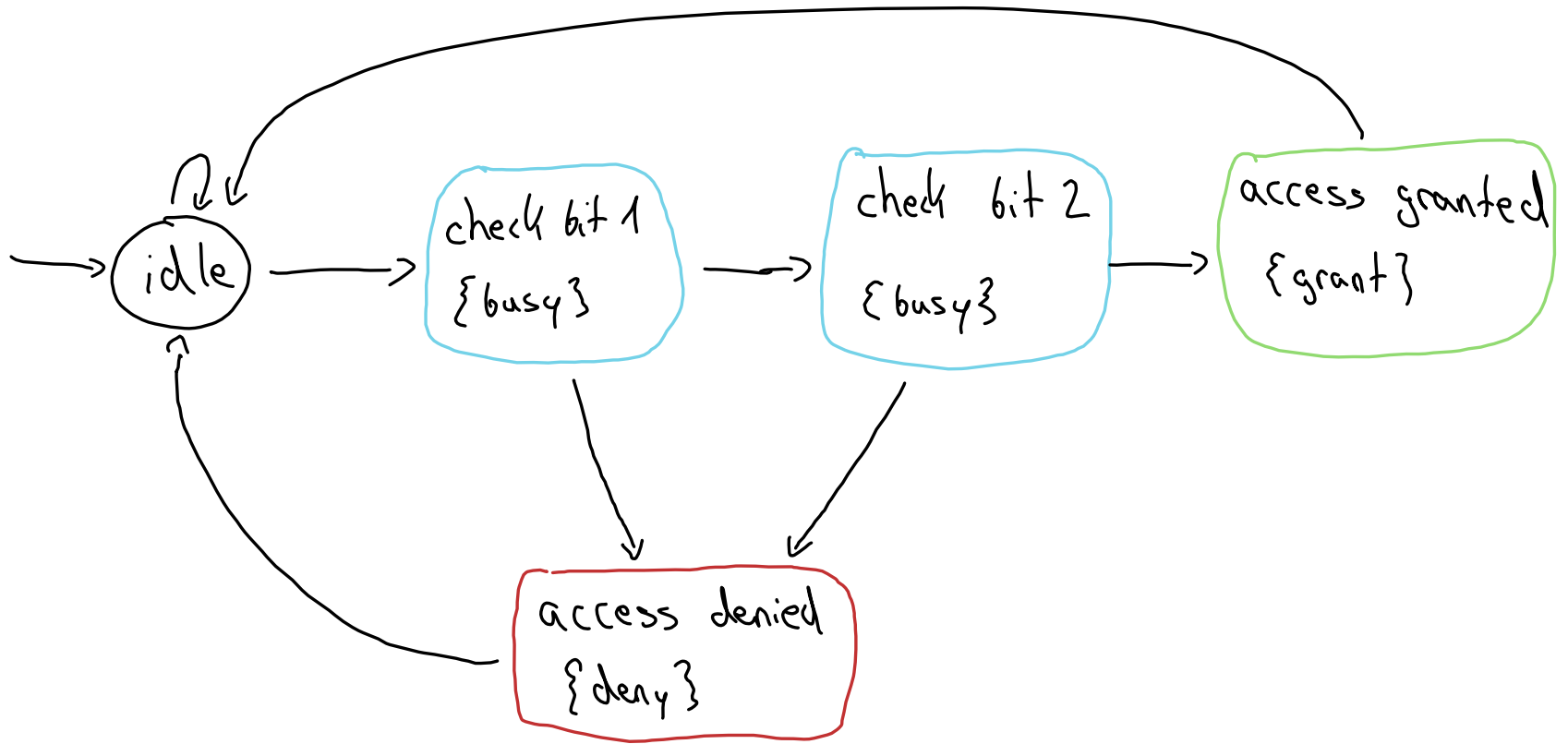
$G (\text{busy} \Rightarrow \neg (\text{grant} \vee \text{deny}))$

- Check before grant

$G ((\neg \text{grant}) \Rightarrow \text{busy})$



The program is correct, but is it secure?



trace π : guess 11, secret 00

idle $\rightarrow$ busy $\rightarrow$ deny

trace p : guess 01, secret 00

idle $\rightarrow$ busy $\rightarrow$ busy $\rightarrow$ deny

Verifying Security

Security property $\approx$ Property of set of executions

$\approx$ HyperLTL formula

Going Hyper

Extend regular LTL with:

- universal quantification:

$$\forall \pi. \varphi \Leftrightarrow \text{"for all traces } \pi, \varphi \text{ holds"}$$

- existential quantification:

$$\exists \pi. \varphi \Leftrightarrow \text{"there exists a trace } \pi \text{ for which } \varphi \text{ holds"}$$

Non inference*

"the output does not leak any high input"



"for any execution, there exists another with dummy high input and the same observable behaviour"



$$\forall \pi. \exists p. \textcolor{violet}{G} (\neg h_p \wedge (L_\pi = L_p) \wedge (O_\pi = O_p))$$

* McLean, 1994 long title

Non interference*†

"the output is not influenced by high input"

+

"low input need not be deterministic"

$$\forall \pi. \forall \rho. \exists \sigma. \textcolor{violet}{G} \left((h_\pi = h_\sigma) \wedge (L_\rho = L_\sigma) \wedge (o_\rho = o_\sigma) \right)$$

* Goguen & Meseguer, 1982 "Security Policies and Security Models"

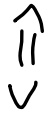
† McCullough, 1988 "Noninterference and the Composability of Security Properties"

Observational Determinism*

"executions with the same low input remain indistinguishable"

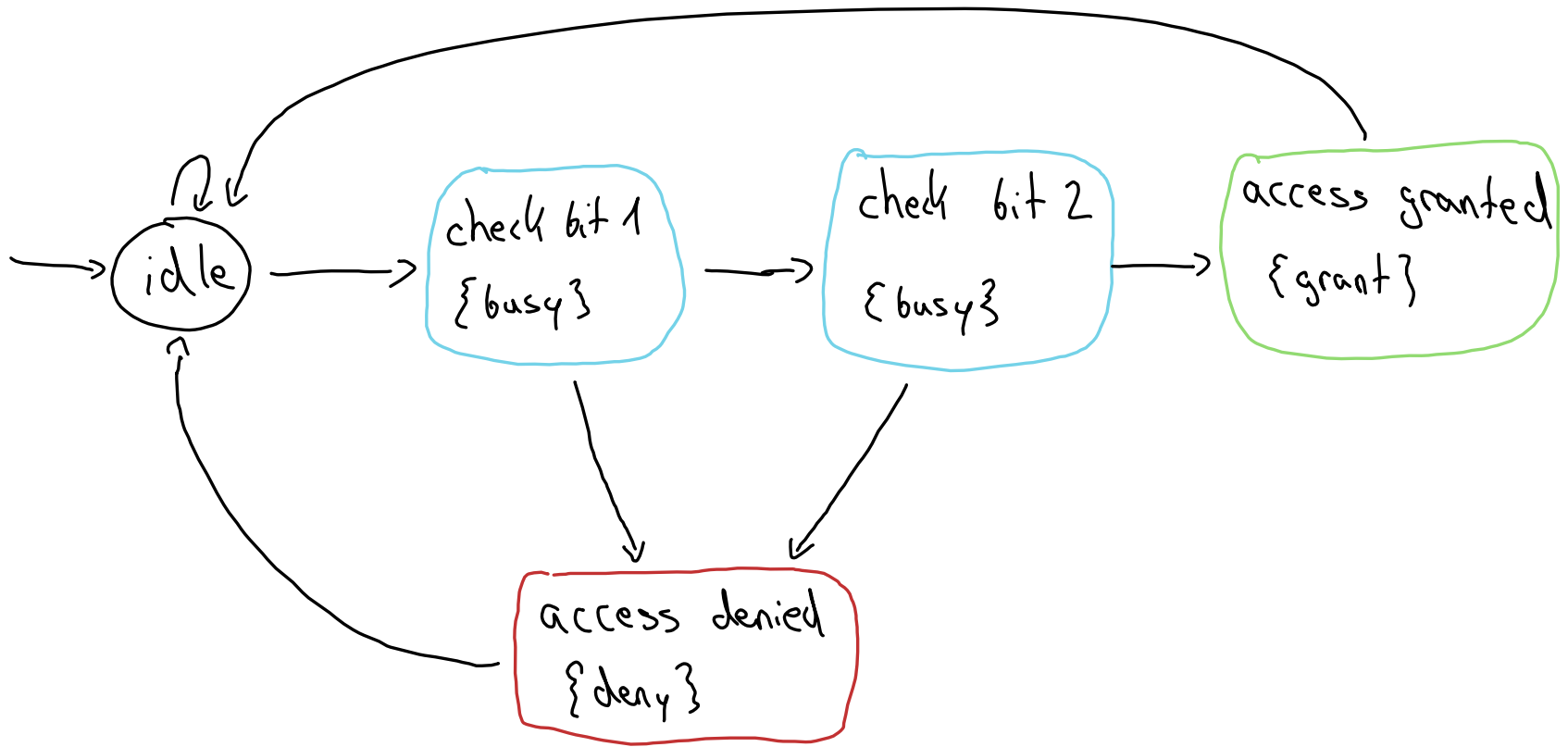


"the program is deterministic to low observers"



$$\forall \pi. \forall \rho. (L_\pi = L_\rho) \Rightarrow G (O_\pi = O_\rho)$$

* Zdancewic & Myers, 2003 "Observational Determinism for Concurrent Program Security"



Noninference?

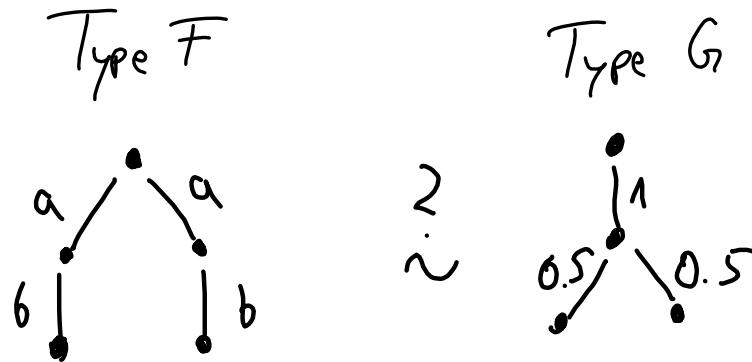
Noninterference?

Observational Determinism?

QUIZ
TIME!

How does this relate to ~~Cybercrime~~?
my work

- Heterogeneous Simulation



~ Binary Logic

Set $F = F$ and reason about pairs of states

This sounds like a $\forall\forall$ hyperproperty!

Further Work

- hyperproperties are based on trace equivalence, not bisimulation
- relate "hyperproperties" expressible in our logic known bisimulation-based notions
- expand on the metatheory for binary logic