Unified Profiling of Attackers via Domain Modeling

Nesrin Hussein[1], Wentao Wang[1], Joseph L. Nedelec[2], Xuetao Wei[3], and Nan Niu[1]

[1]Department of EECS, Univ. of Cincinnati, USA

[2]School of Criminal Justice, Univ. of Cincinnati, USA

[3]School of Information Technology, Univ. of Cincinnati, USA

E-mail: nan.niu@uc.edu

September 12, 2016 @ iRENIC

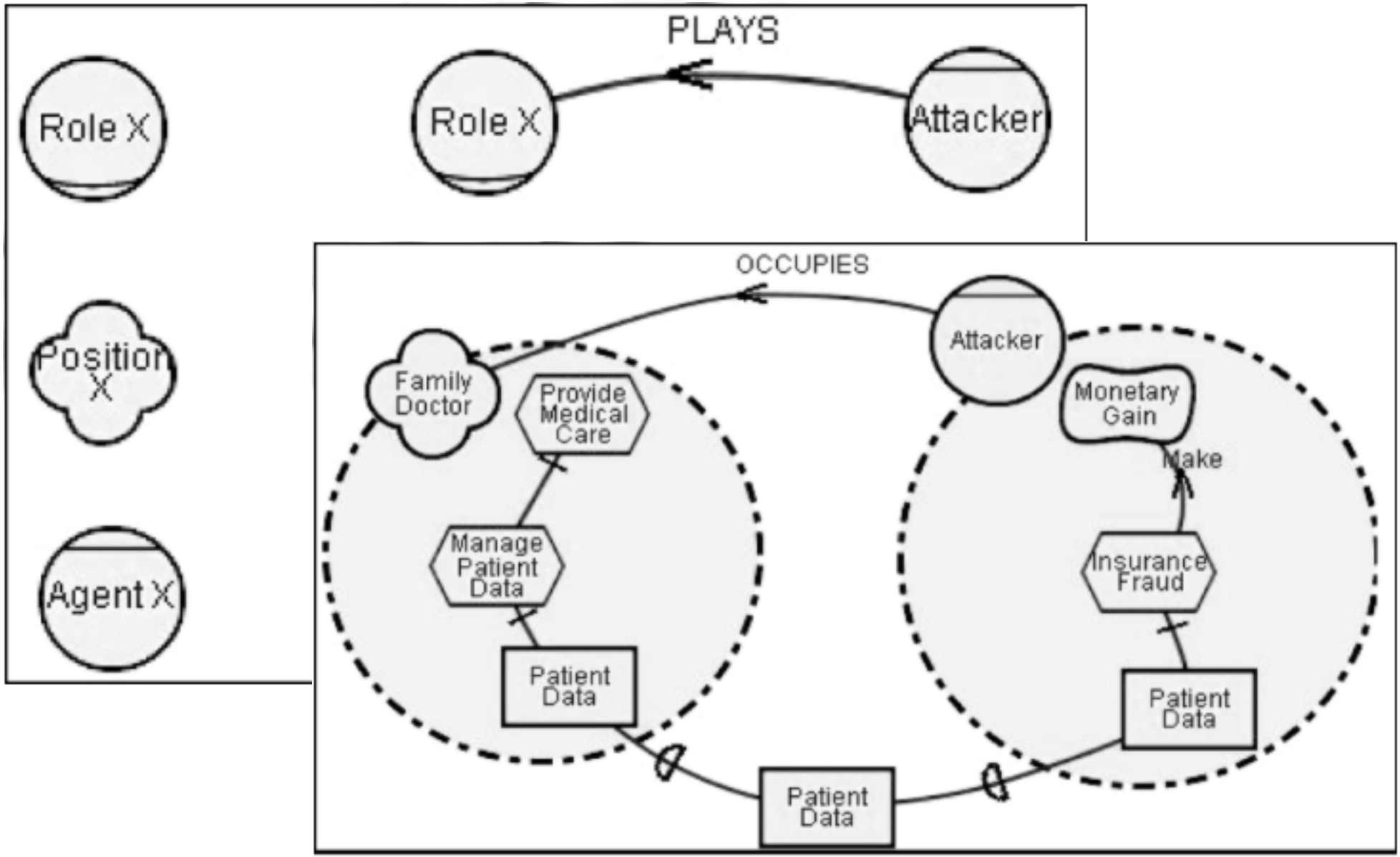
Attackers

- Attacker = a single offender or a group committing the crime

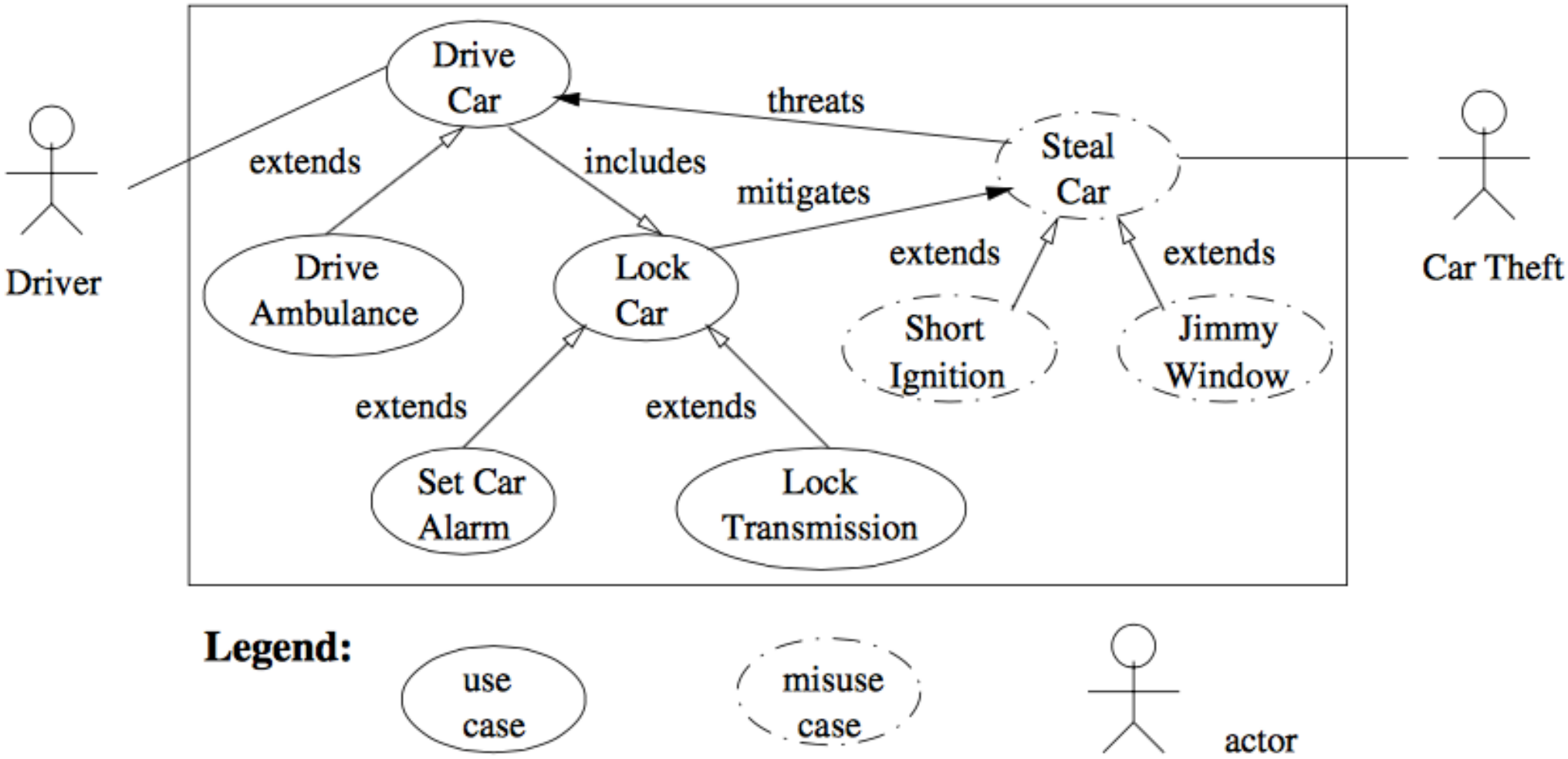
How's attacker modeled in RE?

- Attacker is a (special) kind of stakeholders (those who win or lose from the change introduced by software)

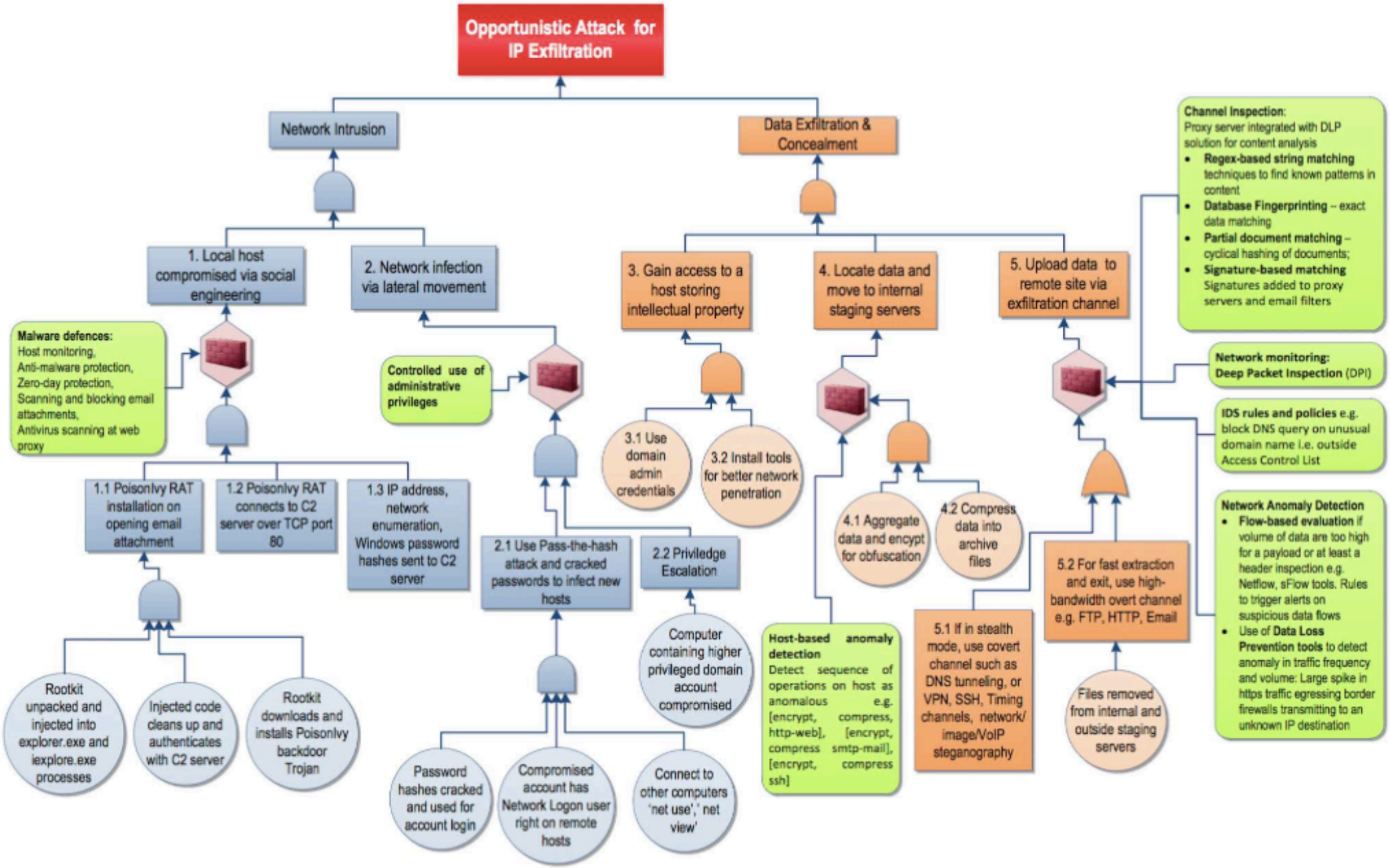
Secure *i** (e.g., Liu-IJSI'09)



Misuse Case (e.g., Sindre-REJ'05)



Incident Fault Trees (e.g., Rashid-ICSE'16)



Consideration of Attacker in RE

⇨Not always modeled

⇨When modeled, done in a fragmented way

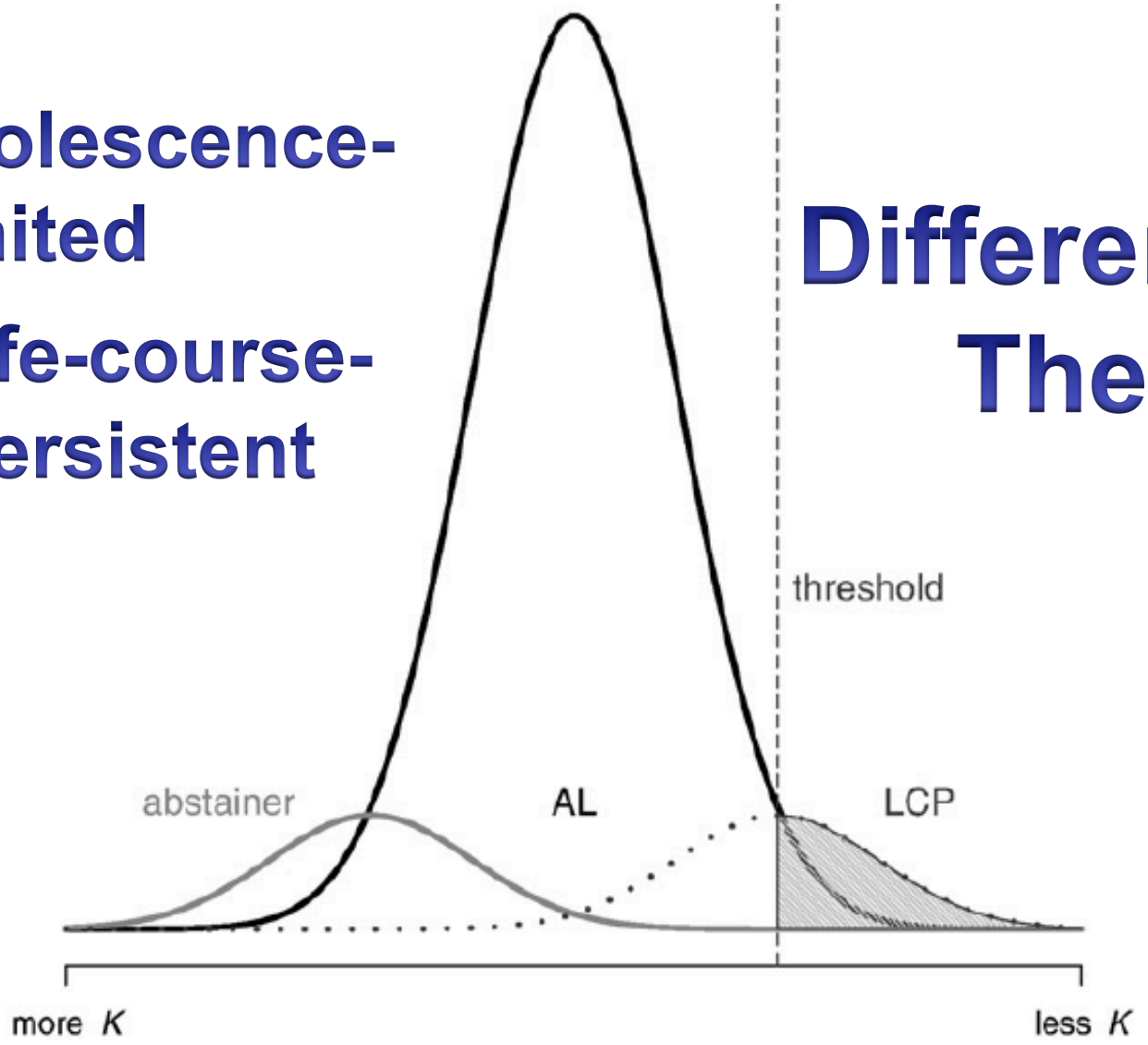
⇨Unifiable via criminology?

Boutwell *et al.*, 2015

A unified crime theory: The evolutionary taxonomy

AL: adolescence-limited

LCP: life-course-persistent



Differential-K Theory

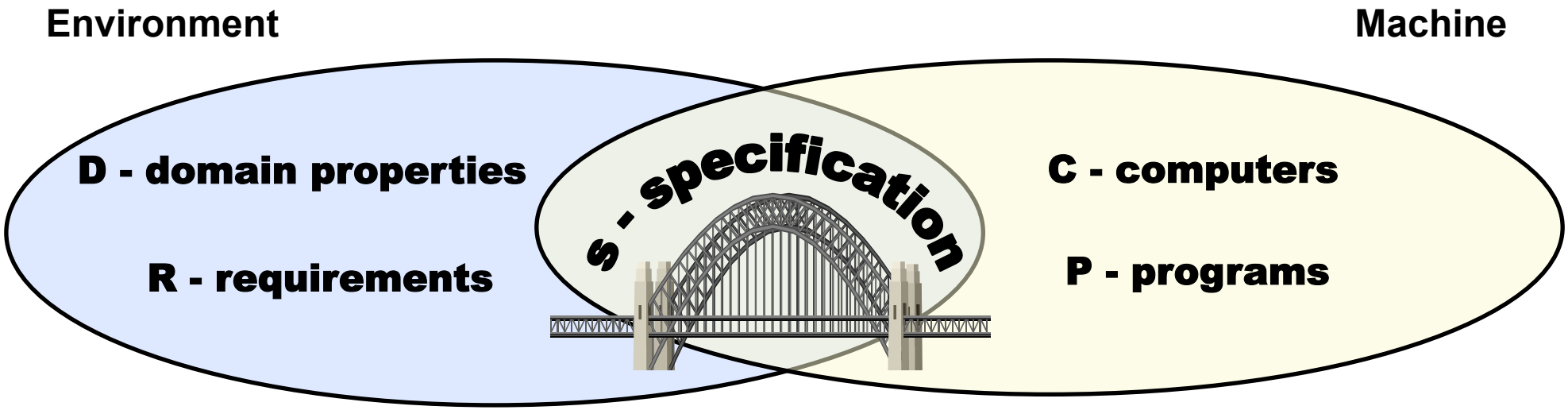
A Unified Theory: origins of criminal behaviors

⇨Basic tenets/predictions about "origins of criminal behaviors" lie in:

deviating from *K* (carrying capacity)

⇨Manifestations: race, age, sex, family size (e.g., # of children), family structure (e.g., single parent homes), socioeconomic status, urban residency, etc.

Jackson's "Meaning of Req.s"



P, C |- S

D, S |- R

("|-" means entailment)

Extending Jackson's Conceptualization

V, C |- A

D, A |- R_A

("|-" means entailment)

Our Hypothesis

⇨ The degree of knowledge that the attacker has about the environment will be reflected in D:

more advanced understanding D is ➔
more likely the attacker's attack is successful

Is Our Hypothesis Sensible?

- An initial manual analysis of 7 CVE (cve.mitre.org) injection attacks reported from 1/1/2015 to 6/27/2016
- Wanted explicit attacker info./ID
- Mapped D value to the types of domain knowledge exploited in the attack

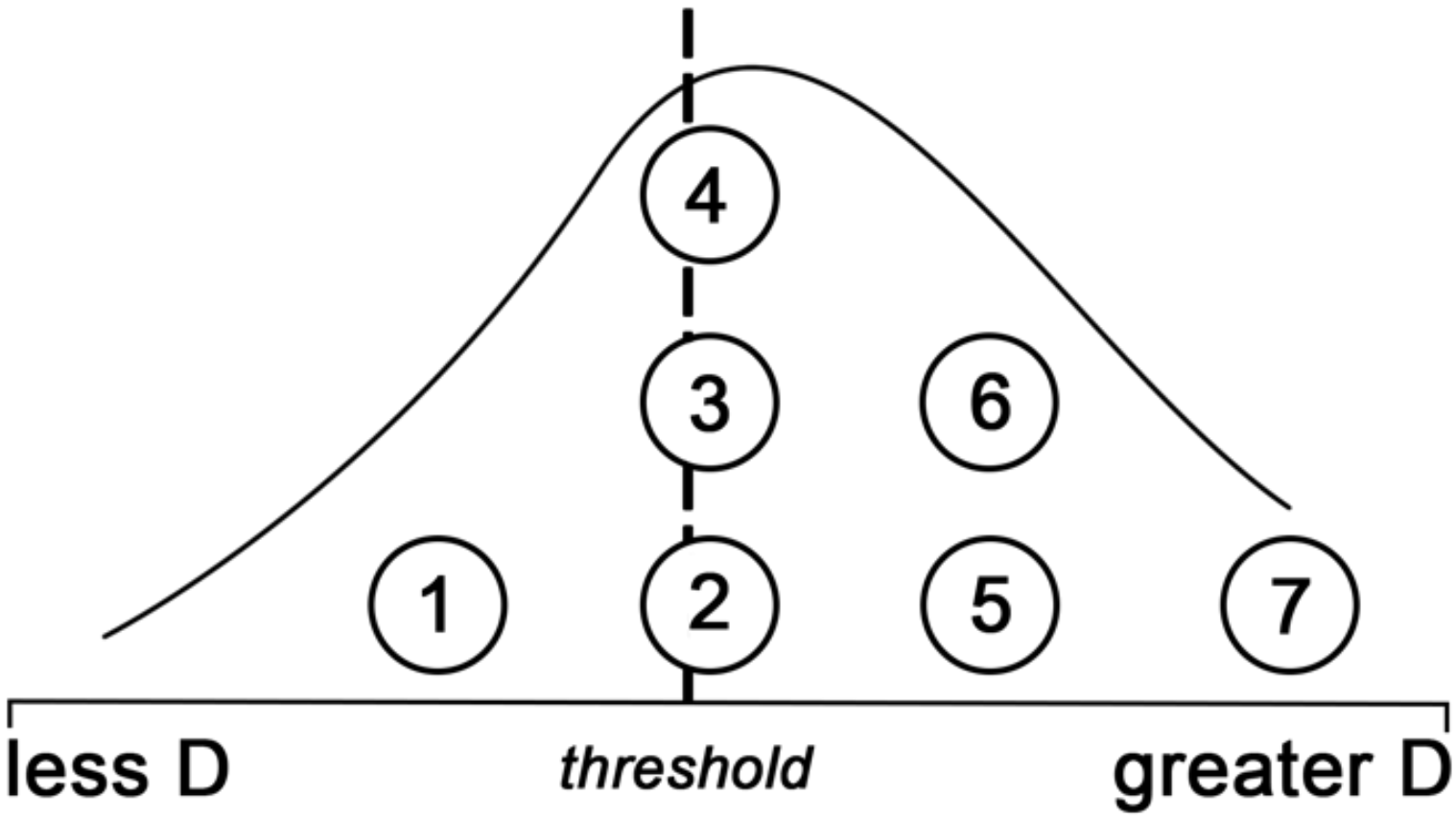
Attack and Attacker

ID	Attack (A)	Attacker
①	Blind injection in WordPress	Larry Cushdoller
②	SQL injection 1 in Cacti	Paul Gevers
③	SQL injection 2 in Cacti	Paul Gevers
④	SQL injection 3 in Cacti	Paul Gevers
⑤	SQL injection in WordPress	Larry Cushdoller
⑥	Command injection in WordPress	Larry Cushdoller
⑦	SQL injection 4 in Cacti	Xin Wang

D and Success

Domain knowledge (D)[1]	D value	Report date (CVE ID[2])
(a)	1	Nov 09, 2015 (--)
(b), (c)	2	Nov 09, 2015 (--)
(b), (c)	2	Jan 4, 2016 (2016-2313)
(b), (c)	2	Mar 10, 2016 (2016-3172)
(b), (c), (d)	3	Jun 21, 2015 (2015-4694)
(a), (c), (e)	3	Dec 2, 2015 (2015-7527)
(a), (b), (c), (f)	4	Jun 9, 2015 (2015-4342)

D as a Unifier



Open Challenges

- ⇨ Better instantiate D (e.g., hiddenness, tech savvy,, what's to do & what's not)
- ⇨ Better instantiate the D-induced distribution (e.g., severity of the attack)
- ⇨ More attacker profiles & attacker's self-evolution

Unified Profiling of Attackers via Domain Modeling

Thank You!