

Unified Profiling of Attackers via Domain Modeling

Nesrin Hussein¹, Wentao Wang¹, Joseph L. Nedelec²,
Xuetao Wei³, and Nan Niu¹

¹Department of EECS, Univ. of Cincinnati, USA

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

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

E-mail: nan.niu@uc.edu

September 12, 2016 @ iRENIC

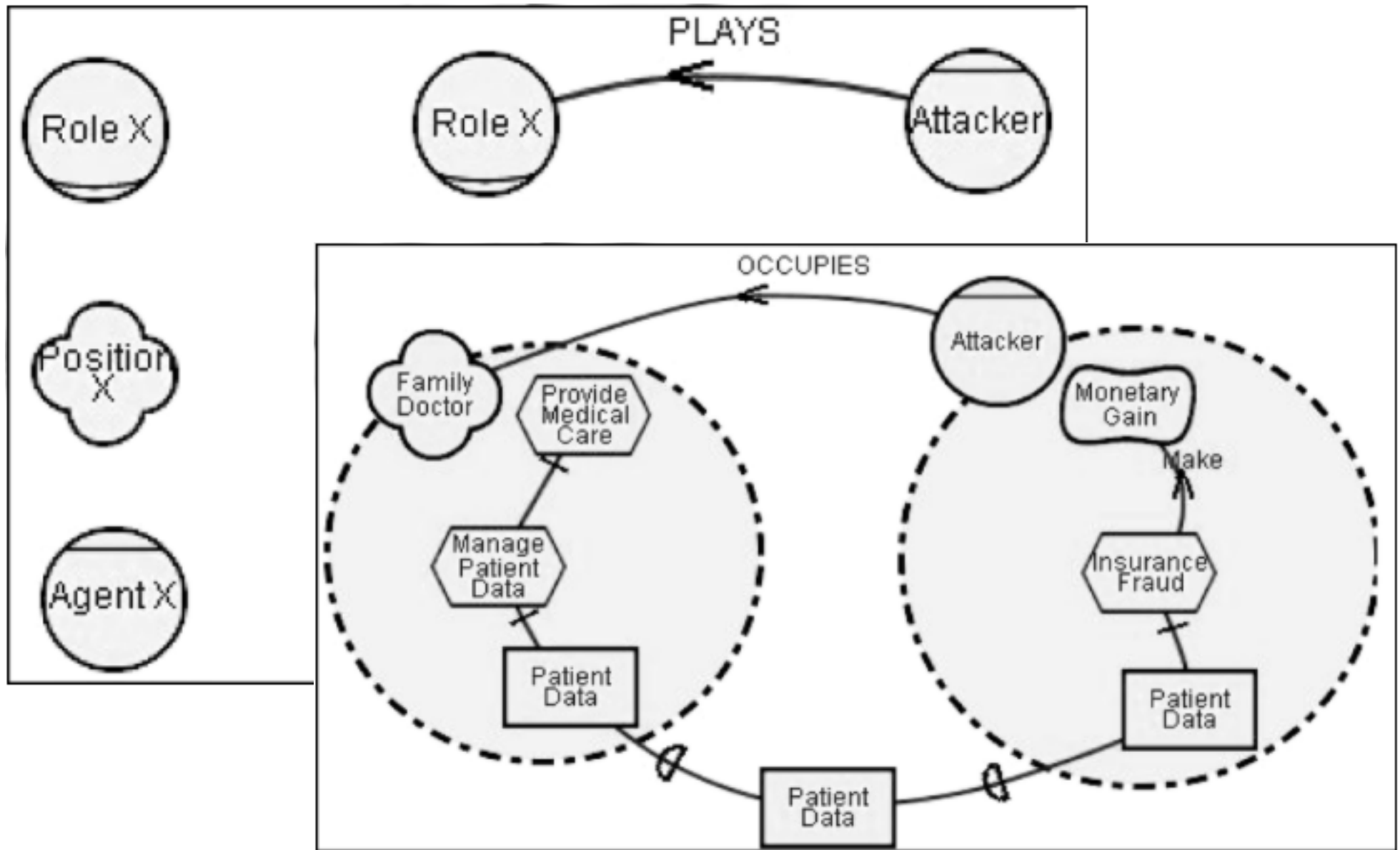
Attackers

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

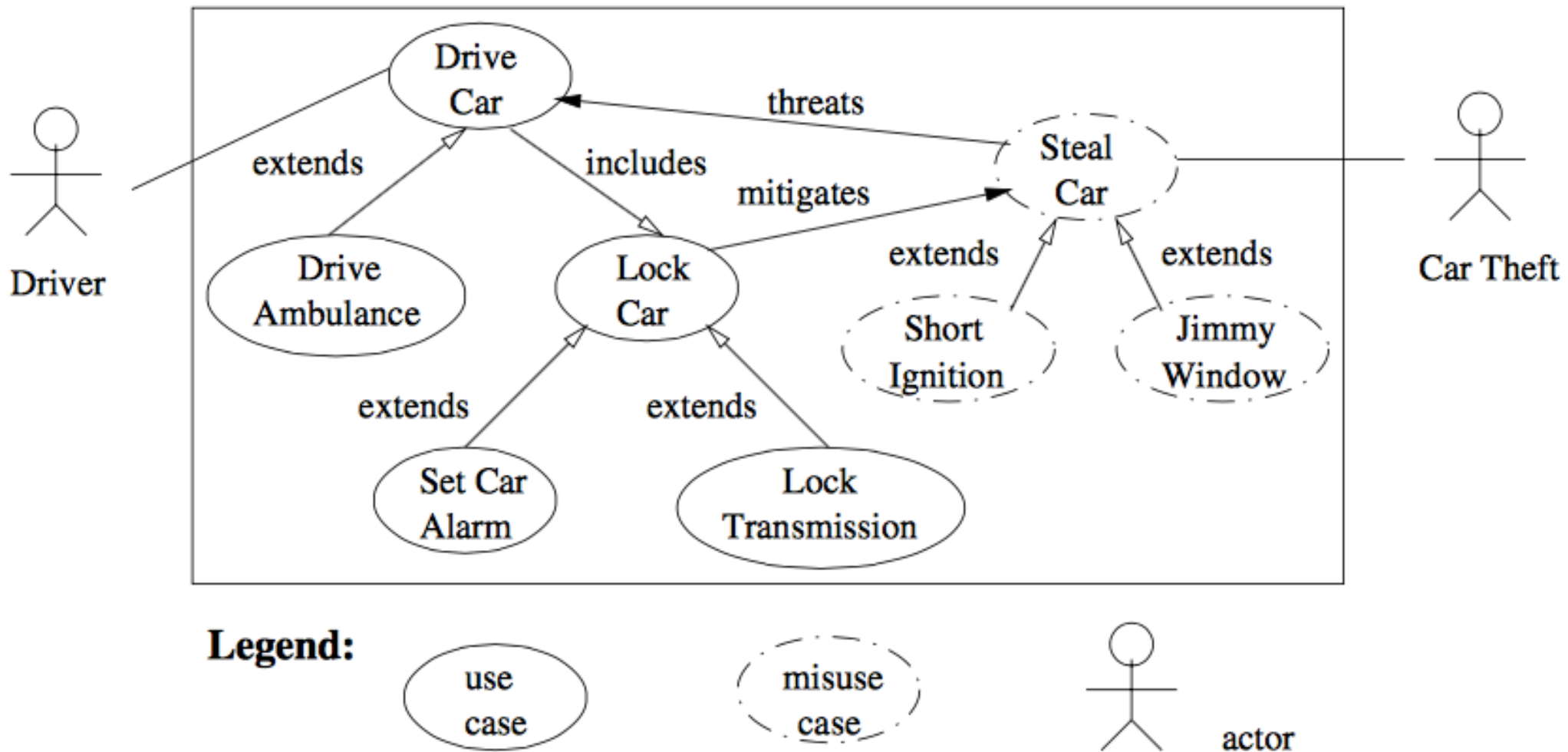
How's attacker modeled in RE?

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

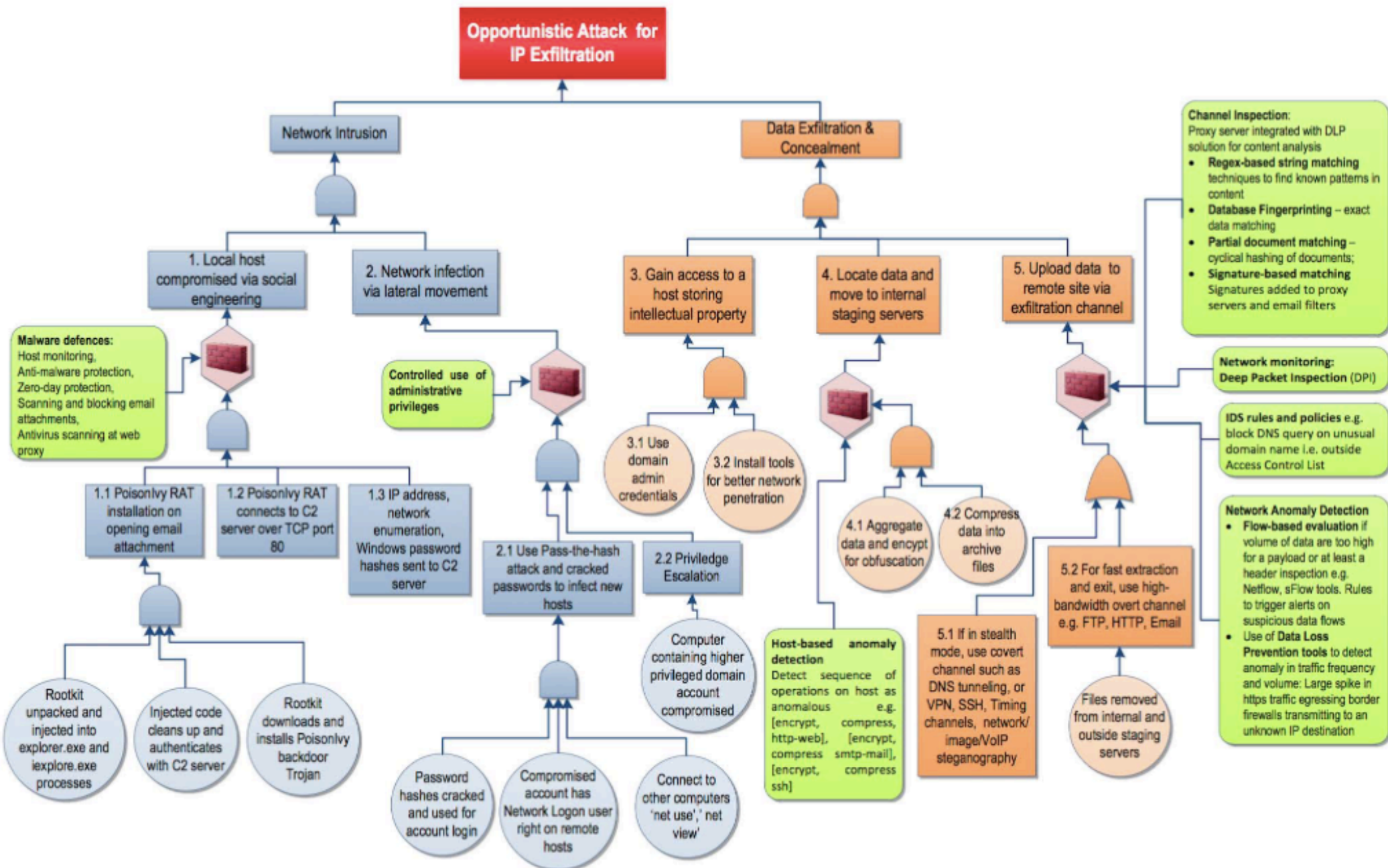
Secure i^* (e.g., Liu-IJSI'09)



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



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



Malware defences:
Host monitoring,
Anti-malware protection,
Zero-day protection,
Scanning and blocking email attachments,
Antivirus scanning at web proxy

Controlled use of administrative privileges

Host-based anomaly detection
Detect sequence of operations on host as anomalous e.g.
[encrypt, compress, http-web], [encrypt, compress smtp-mail], [encrypt, compress ssh]

Channel Inspection:
Proxy server integrated with DLP solution for content analysis

- **Regex-based string matching** techniques to find known patterns in content
- **Database Fingerprinting** – exact data matching
- **Partial document matching** – cyclical hashing of documents;
- **Signature-based matching** Signatures added to proxy servers and email filters

Network monitoring: Deep Packet Inspection (DPI)

IDS rules and policies e.g.
block DNS query on unusual domain name i.e. outside Access Control List

Network Anomaly Detection

- **Flow-based evaluation** if volume of data are too high for a payload or at least a header inspection e.g. Netflow, sFlow tools. Rules to trigger alerts on suspicious data flows
- **Use of Data Loss Prevention tools** to detect anomaly in traffic frequency and volume: Large spike in https traffic egressing border firewalls transmitting to an unknown IP destination

5.1 If in stealth mode, use covert channel such as DNS tunneling, or VPN, SSH, Timing channels, network/ image/VoIP steganography

Files removed from internal and outside staging servers

5.2 For fast extraction and exit, use high-bandwidth overt channel e.g. FTP, HTTP, Email

3.1 Use domain admin credentials

3.2 Install tools for better network penetration

4.1 Aggregate data and encrypt for obfuscation

4.2 Compress data into archive files

3. Gain access to a host storing intellectual property

4. Locate data and move to internal staging servers

5. Upload data to remote site via exfiltration channel

Data Exfiltration & Concealment

Network Intrusion

Opportunistic Attack for IP Exfiltration

Consideration of Attacker in RE

⇒ Not always modeled

⇒ When modeled, done in a fragmented way

⇒ Unifiable via criminology?

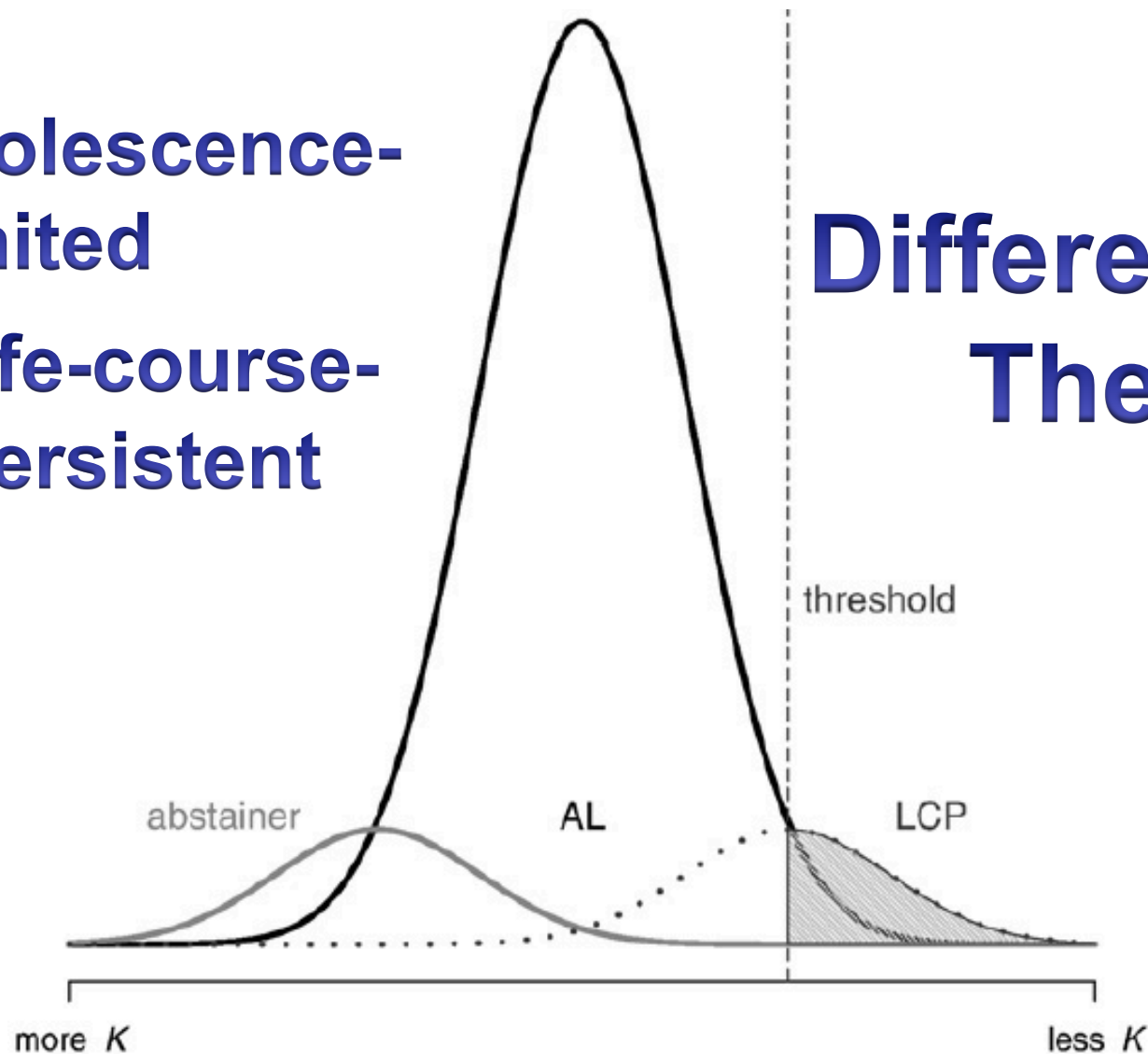
Boutwell *et al.*, 2015

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

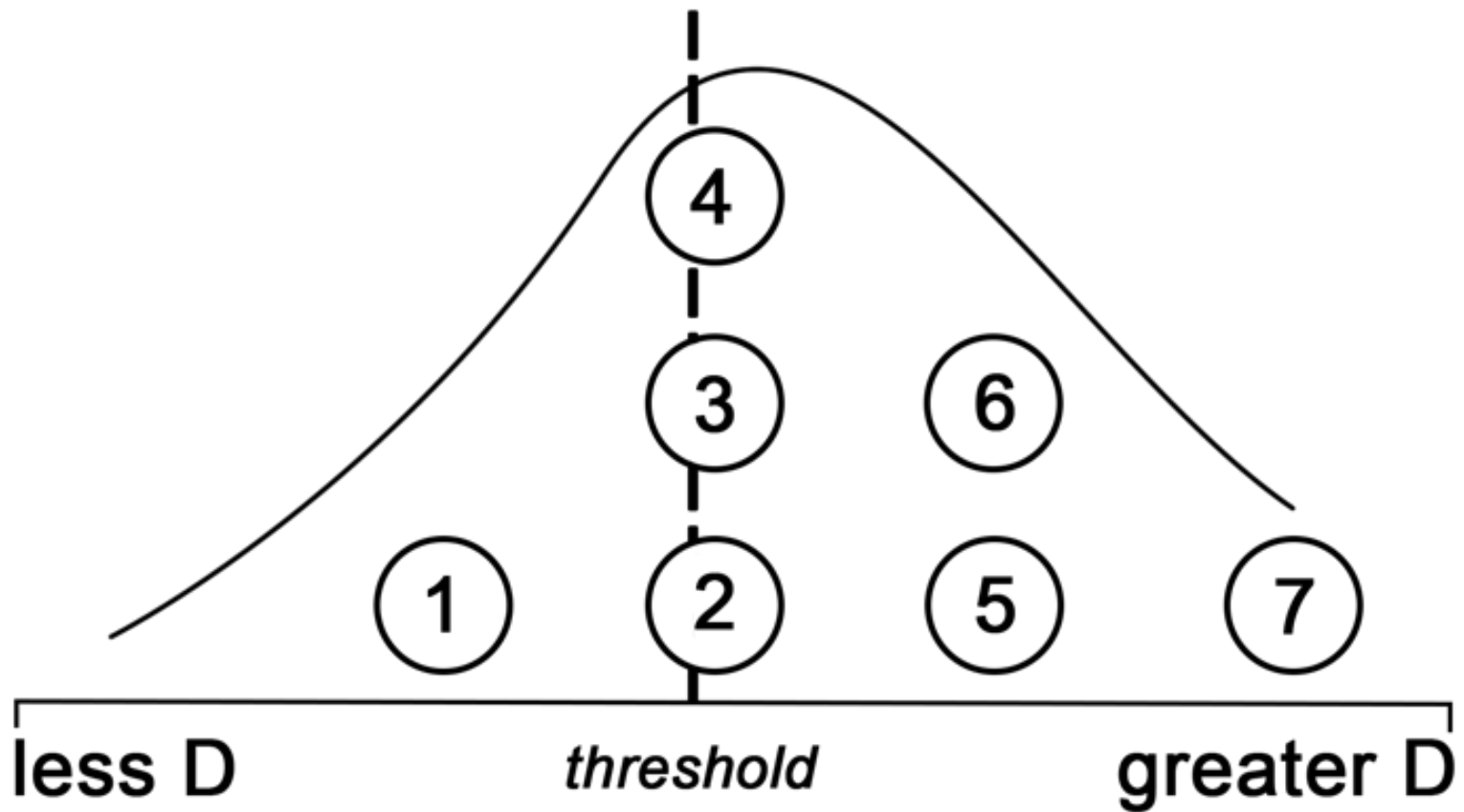
Attack and Attacker

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 ID²)
(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!

