Enhanced Dooley Graphs for Modeling, Analyzing, and Attributing Ransomware Attacks

PI: H. Van Dyke Parunak, Ph.D., ABC Research, LLC

> www.abcresearch.org/papers/dooldesn.pdf, www.abcresearch.org/papers/dooley.pdf

## **Ransomware Distinctives:**

#### **Requirements:**

- Unambiguous, formal model of interaction
- Understandable by human analysts
- Victim knows of attack while in progress
- Victim and attacker interact deliberately
- Outcome depends on collaboration
- → Compare formalisms for E-commerce

## Tractable for computer modeling

# **Dooley Graphs**

- Invented by field linguists to study discourse
- Widely used since 1996 in E-commerce

# **Building Blocks for Transactions**

Physics

Biology

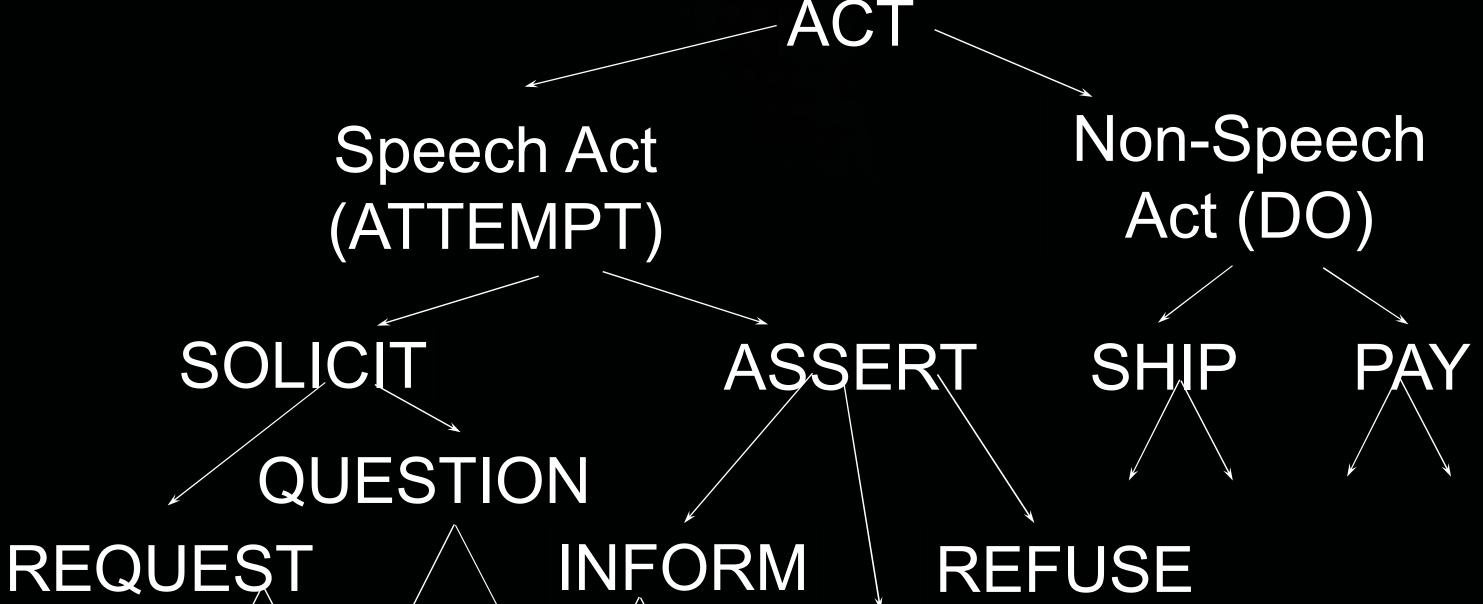
Linguístics

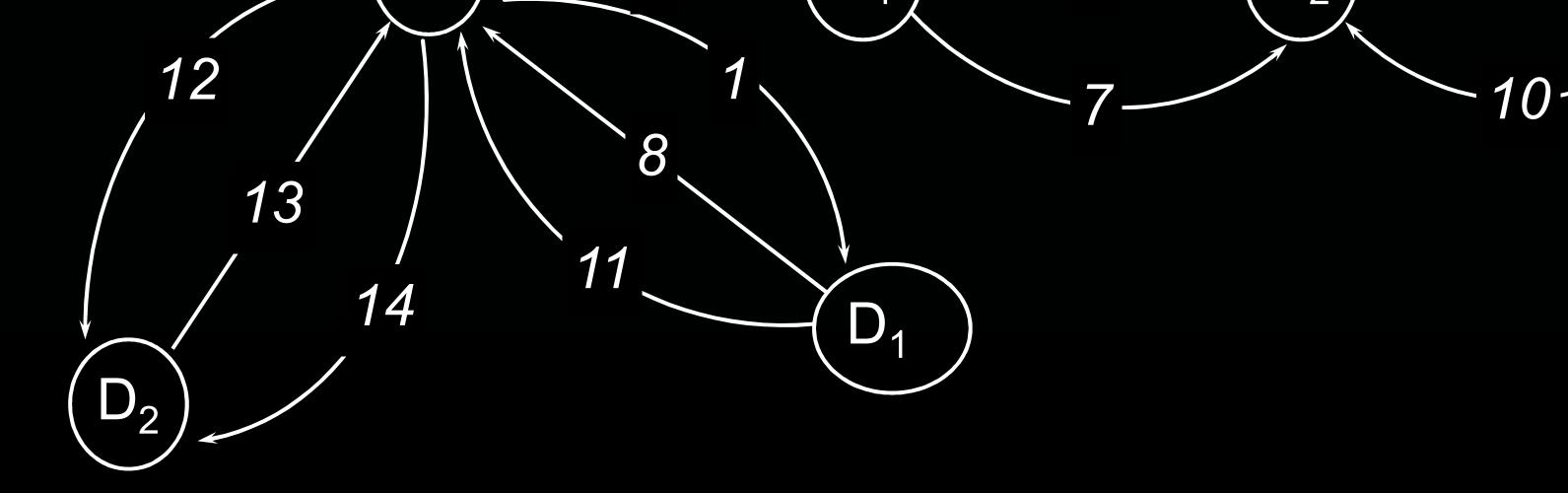
ABC Research, LLC

	Responds	Replies	Resolves	Completes
I Evamnia I	Any	Any	Question-	Commitment-
	sequence	interchange	Answer	Execution
Relation	Causal	Causal	Causal + "obeys"	Causal + fulfills
Speakers	Any	Reciprocal	Reciprocal	Same
Control		Undefined	Same	Same

#### **Dooley Graphs and Other Discourse Formalisms** COMMIT Node = Participant Participants: (x Role) Who is **Example Dooley Graph in E-Commerce** speaking to Edge Whom? connectivity Node = $C_3$ BA Utterance State (Participant x) Role B Graph: Diagram: How do the What is each utterances fit speaker's together? State? $C_2$ 6 $A_2$

# Speech Act Theory (Austin 1962; Cohen and Levesque 1995; Parunak 1996

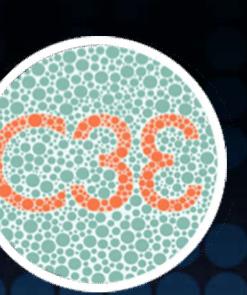






/个\

SPECIAL CYBER OPERATIONS RESEARCH AND ENGINEERING



Proposal:

- Develop Dooley Graph mapping for ransomware domain
- Construct Dooley Graphs for actual cases
- Identify distinguishing features
- Merge into Dooley Graph of potential interactions
- Demonstrate usefulness for attribution, prediction, and PIR generation

**Computational Cybersecurity in Compromised Environments** 2016 Fall Workshop | October 17-19 | Atlanta, Georgia