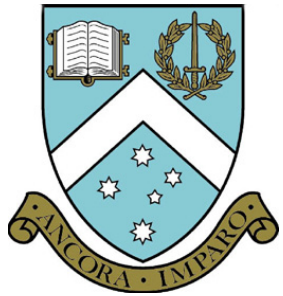


The Analysis of Compound Information Warfare Strategies

Dr Carlo Kopp, MIEEE, MAIAA, PEng
carlo@csse.monash.edu.au
Clayton School of Information Technology
Monash University, Clayton 3800, Australia

Abstract

- ***Practical defensive and offensive application of Information Warfare most frequently involves the use of complicated compound strategies, in which multichannel and multilayered attacks must be analysed.***
- ***This paper presents a systematic approach to the analysis problem, which is exploitable for defensive and offensive purposes.***

The Four Canonical Strategies of InfoWar

- **Degradation or Destruction [also Denial of Information]**, i.e. concealment and camouflage, or stealth; Degradation or Destruction amounts to making the signal sufficiently noise-like, that a receiver cannot discern its presence from that of the noise in the channel.
- **Corruption [also Deception and Mimicry]** , i.e. the insertion of intentionally misleading information; corruption amounts to mimicking a known signal so well, that a receiver cannot distinguish the phoney signal from the real signal.
- **Denial [also Disruption and Destruction],** i.e. the insertion of information which produces a dysfunction inside the opponent's system; alternately the outright destruction of the receiver subsystem; Denial via disruption or destruction amounts to injecting so much noise into the channel, that the receiver cannot demodulate the signal.
- **Denial [also Subversion]** , i.e. insertion of information which triggers a self destructive process in the opponent's target system; Denial via subversion at the simplest level amounts to the diversion of the thread of execution within a Turing machine, which maps on to the functional behaviour of the victim system, i.e. surreptitiously flipping specific bits on the tape, to alter the behaviour of the victim Turing machine.

Problems?

- Understanding and analysing a complex compound deception strategy. Such a strategy can comprise a very larger number of canonical primitives.
- Properly understanding the structure of the strategy, and thus its underlying aims, can present difficulties.
- Example: an opponent is playing a very complex compound deception strategy. The aim of the defender is to determine whether gathered information is a deception or not, and what the specific aim of that deception might be. In the simplest of terms, ‘what does this opponent want me to think and why?’
- Detection of inconsistencies, mistakes or gaps in such a complex deception strategy may be the only method of unmasking such a deception, especially if the deception is carefully architected from the outset.

Problems (Cont)

- Another problem which can frequently arise is that of countering an opponent's deceptive perception management strategy.
- Such deceptions can often be complex compound strategies in which multiple mutually reinforcing falsehoods are employed with a specific aim of shifting the perceptions of a victim audience.
- Often the only technique for defeating such a strategy is to unmask the deception before the audience.
- A well crafted compound strategy may present genuine difficulties in analysis and defeat.

Primitives , Precedence, Compound Strategies

- **The Attacker:** the player in an information warfare strategy who is executing the strategy against a victim player.
- **The Victim:** the player in an information warfare strategy who is being subjected to an attack by the attacking player.
- **Canonical Strategy:** defined as one of the four fundamental strategies. These strategies are atomic, in the sense that any compound strategy can be divided into a number of canonical strategies, but a canonical strategy cannot be further divided in any way.
- **Compound Strategy:** any strategy which comprises more than one canonical information warfare strategy, and in which some defined precedence relationship exists between these strategies.

Precedence Relationships

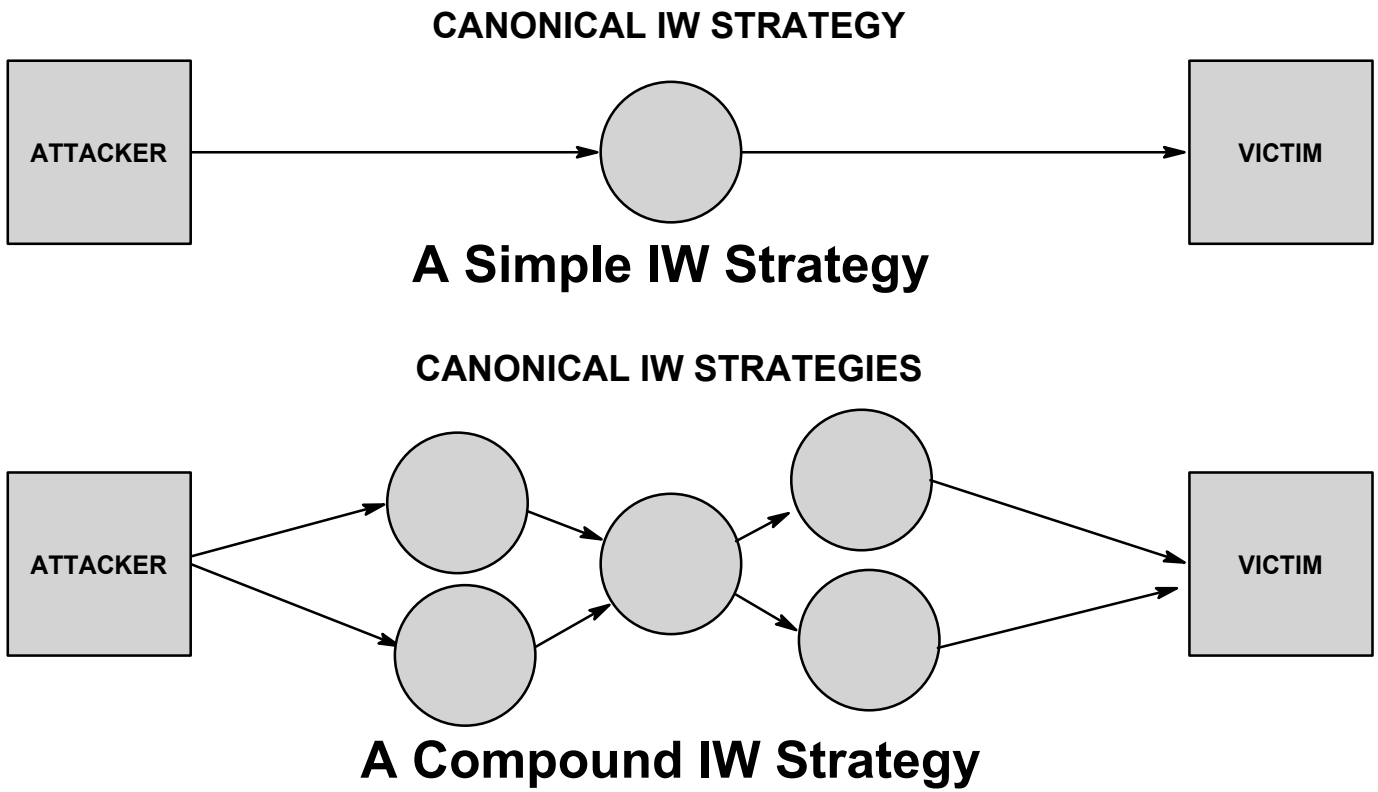
- **Precedence Relationships:** define the order or precedence which exists between more than one canonical information warfare strategy comprising a compound strategy:

1. In practical terms, one canonical strategy can be a precedent to one or more canonical strategies.
2. The precedence relationship cannot be bidirectional since the time domain is not bidirectional.
3. It is only once the precedent strategy has achieved some effect, that the antecedent strategy can produce its effect.
4. There is no bound on the number of precedent strategies to any antecedent strategy.

Precedence Relationships (Cont)

5. Precedence is unidirectional in time, therefore any compound strategy forms a directed graph, which obeys the properties of directed graphs.
6. Precedence relationships arise due to the state of the victim in the attack. In a compound strategy, antecedent strategies may not be feasible until a specific state of misperception or false belief has been established in the victim. A strategy may only be successful if this state change has taken place.
7. An attacker may or may not perceive the state change in the victim's perception arising from an attack, compound or simple, and thus execute an antecedent strategy, compound or simple, after executing the precedent attack. This may or may not impair the success of the antecedent attack.

Simple vs Compound IW Strategies



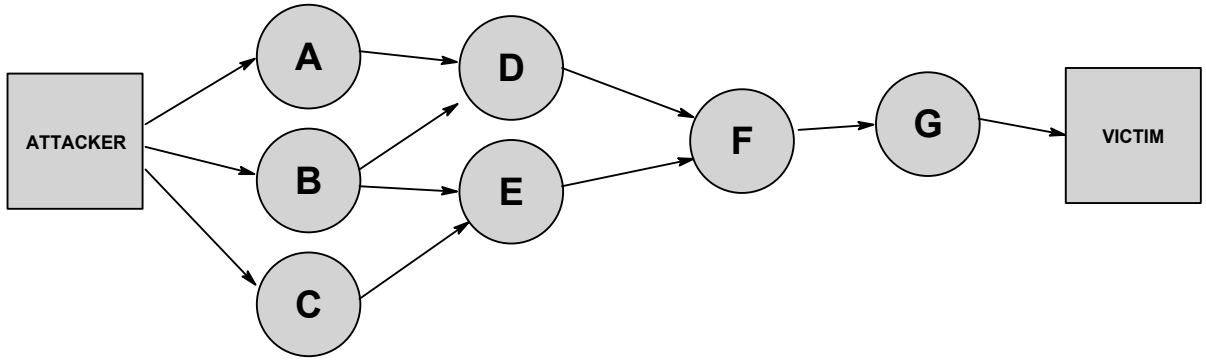
Primitives (Cont)

- **Concurrency:** Strategies between which no precedence relationship exists can be executed concurrently. There is no bound on the number of possible concurrent strategies.
- **Primary vs Supporting Strategies:** A strategy is said to be a supporting strategy if it supports the aim of another strategy, termed the primary strategy.
  1. Supporting and primary strategies may or may not be concurrent.
  2. A non-concurrent supporting strategy is a strategy which must produce its effect before the primary strategy can be executed successfully.

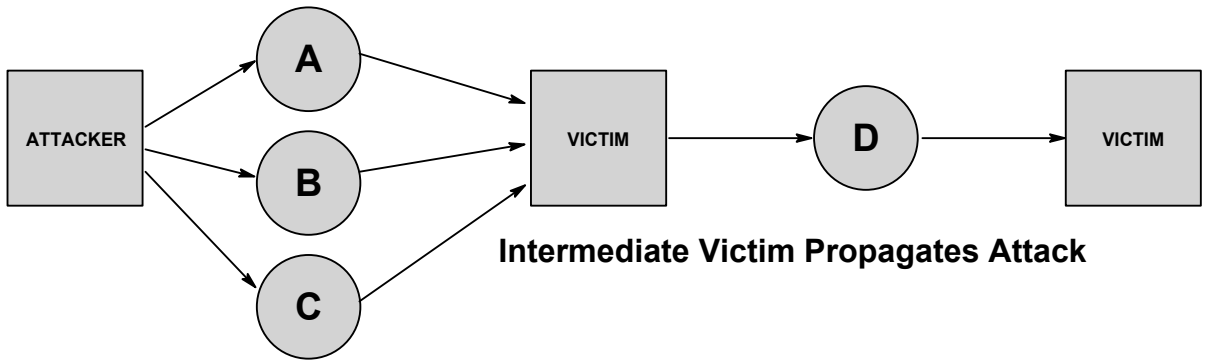
Primitives (Cont)

- **Chained or Sequential Strategies:** a compound strategy in which one or more intermediate victims are exploited. In such a strategy the first victim is employed as a conduit or proxy to propagate an information warfare attack, or its effect.
  - Example: exploitation of media organizations by terrorist movements. The media organization is deceived into propagating a message targeted at a victim population, believing the message constitutes legitimate news.
- **Victim State:** defined as the victim's belief at that point in time.
  - A successful application of information warfare will effect an intended state change.
  - An unsuccessful application may not produce a state change, or may by alerting the victim, produce a state change in whatever other game the victim may be playing.

Chained Compound vs Compound Strategies



A Compound IW Strategy



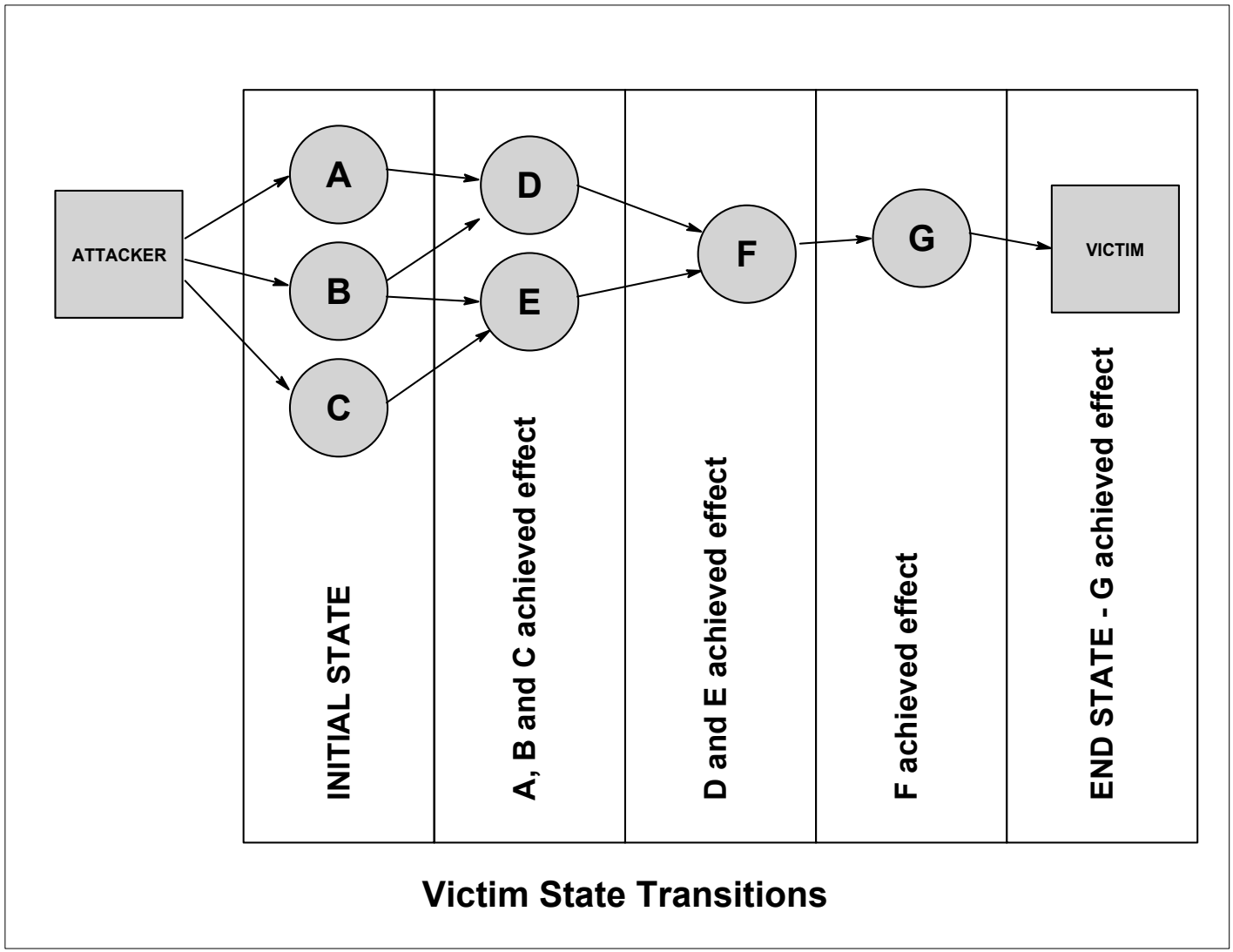
Intermediate Victim Propagates Attack

A Chained Compound IW Strategy

MODELLING COMPOUND STRATEGIES

- A model for a complex compound strategy is a directed graph, in which precedence relationships exist between component canonical strategies.
- The topology of this graph is dependent upon the structure of the compound strategy.
- The overall success of any complex compound strategy is measured by the end state of the victim. If the intended end state is not achieved, the strategy has failed.
- In terms of systematically constructing a compound information warfare strategy, the starting point is the end state of the victim, and the intermediate states the victim must transition between from its initial state.

State Transitions



Victim State Transitions

Forensic Analysis

- The *a posteriori* or forensic analysis of past attacks relies on establishing the precedence relationships and achieved states in the victim.
- The order in which specific compound or simple strategies were executed by the attacker is perhaps the most valuable tool the analyst has, as this allows attacks to be grouped, upon which the concurrent canonical strategies can be separated.
- The remaining step is to establish the specific aims of each of the constituent canonical and compound strategies.

Cut Vertices

- As compound information warfare strategies have the properties of directed graphs, the behaviour of the cut vertex is of particular interest.
- A cut vertex is such a vertex, the removal of which partitions the graph into two smaller graphs (Chartrand, 1977; Wilson, 1985).
- Any strategy, canonical or compound, which possesses the cut vertex property is a vulnerability within the overall compound information warfare strategy.
- The failure of this particular strategy, or its defeat by the victim, results in the total failure of the whole strategy.
- *Cut vertices are thus a critical vulnerability in compound Information Warfare strategies.*

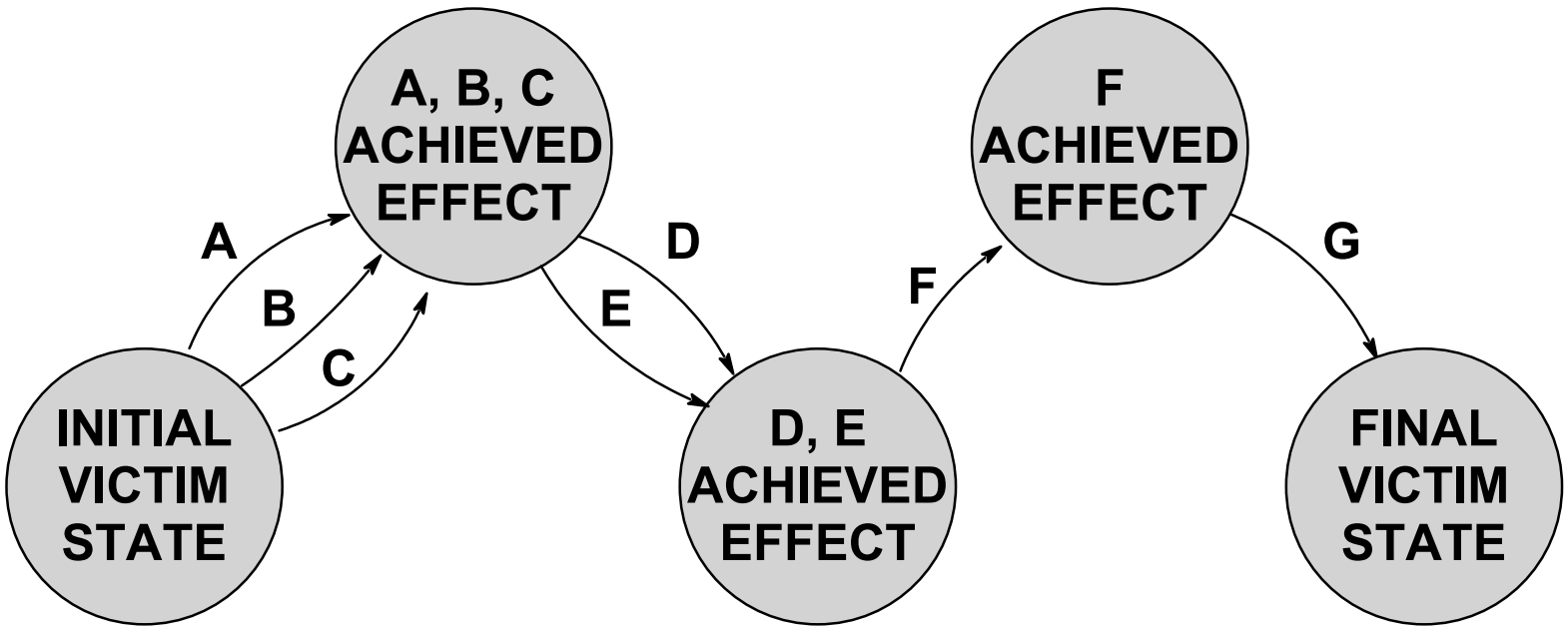
Robustness of Compound Strategies

- The attacker can assess the robustness of the strategy at each state transition, by identifying whether the required strategies to effect that state transition have the cut vertex property, and thus represent a single point of failure for the strategy.
- Robustness could be improved by executing two or more concurrent compound strategies, all of which effect the same end state in the victim.
- This is an application of the established reliability engineering technique of ‘parallel redundancy’ (Bazovsky, 1961).
- Example: 1944 Fortitude operation (Ministry of Defence, 2004; Ricklefs, 1996).

STATE BASED MODELLING

- Alternate mappings for this modeling technique exist.
- A state based mapping is an alternative - attractive to users familiar with state transition diagrams, or project scheduling techniques such as PERT (Project Evaluation and Review Technique).
- In a state based representation, the graph comprises nodes which represent initial, intermediate and end states for the victim, and directed edges which represent the strategies required to effect a transition from a preceding state.
- Rather than searching for cut vertices in the directed graph, analysis requires that *bridges* be identified (Chartrand, 1977; Wilson, 1985).

State Based Representation



State Based Representation for Compound Strategies

VALIDATION OF MODELS

- Two basic scenarios for validating a model:
  1. Validating a model of a strategy *in progress*.
  2. Validating *a posteriori* a past strategy.
- The first case is usually much more difficult due to incompleteness of data and intentional efforts to conceal the nature of the strategy by the attacker.
- If intelligence information is available to penetrate defences, then analysis of strategies *in progress* is much simplified.
- Strategies in which information is hidden completely will always present analytical difficulties both *a priori* or *in progress*. This is the essence of *strategic surprise*, as defined in the hypergame framework.
- Without evidence to prove that a deception strategy is underway, it is not feasible to perform analysis.

Validation vs Uncertainty

- With poor data, the evolving strategy under analysis is uncertain.
- Effectively, analysis will require the definition of several alternative models for the compound strategy, all sharing those features which existing data can logically support.
- As the strategy evolves further, alternatives will collapse as actions by the player contradict the respective alternative models.
- The analyst therefore produces a tree structured graph identifying possibilities, and the graph is progressively pruned as incoming data causes specific branches of the tree to collapse.

Conclusions

- A systematic analytical technique for modelling and analysing compound information warfare strategies.
- Compound strategies are modelled as directed graphs, with precedence relationships where applicable.
- Discrete state transitions in the victim used as a measure of success.
- The concept of robustness in a compound strategy is introduced, this being defined as a measure of how few component strategies in the compound strategy possess the cut vertex property.
- Future research is required to further explore techniques for the analysis of attacks *in progress*, techniques for modelling partial effects upon victims, and the effects of belief (false or true) in attackers and victims.