Using Game Theory To Solve Network Security

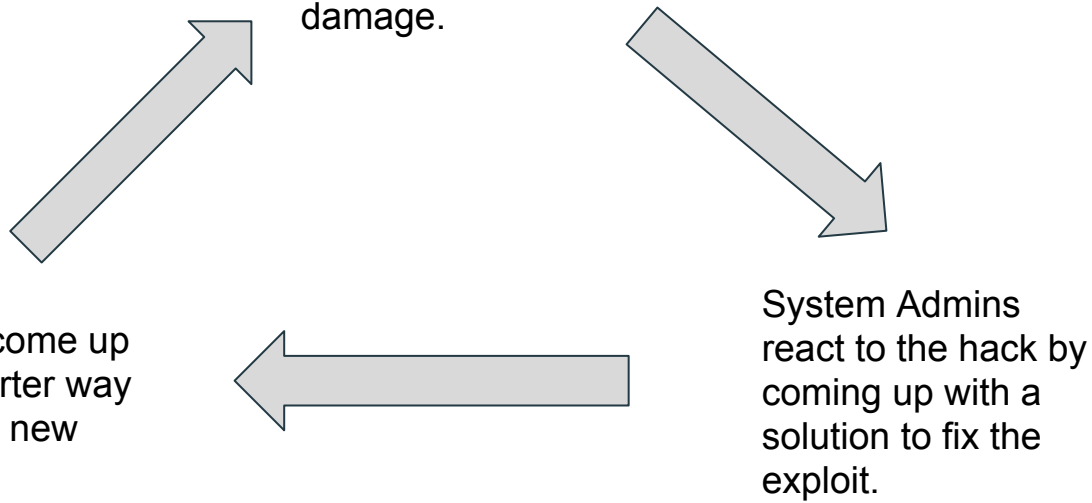
A brief survey by Willie Cohen

Network Security Overview

- By default networks are very insecure
  - Connected to the open internet
- There are a number of well known methods for securing a network
  - Encrypting data
  - Firewalls
  - Authentication
  - Restricted permissions
- BUT, none of the methods are perfect, and issues are common inside as well as between methods

The Problem: network security is hard

Caught in an endless cycle:



Solution: game theory

- If successful, a game theoretic approach to security can…
  - provide a mathematical framework for dealing with network security
  - Can automate the job of human analyst
  - Analyse hundreds of thousands of “what ifs”
  - Sophisticate the decision making processes of network administrators with regard to security

- Basically…. Take network security from an art to a science

Brief Overview: Game Theory

Game Theory: A way of modeling different players choices, based on the effect of other players choices.

Player: entity participating in the game

Action: choice a player makes on their turn

Payoff/Reward: gain (or loss) a player receives after choosing their action

Information: Games can have complete information or incomplete information. Complete means that players know the strategies and payoff of their opponents.

Bayesian Game: game where players have incomplete information (strategies | payoffs) on the other players, but they have a probability distribution.

Nash Equilibrium: the optimal outcome of a game, where each player can receive no incremental benefit from changing actions or strategy (can be more than one).

Game Theory & Network Security

We can model a “game” between an attacker, and a network administrator.

Players: Attacker, Network Administrator

Actions:

For attacker - disrupt network (ddos), plant worm, install sniffer, etc…
For network admin - add sniffer detector, remove compromised account, shut off internet traffic, etc…

Payoff:

For attacker - positive for disruption of network, stolen data. Negative for being stopped, traced….
For network admin - positive for detecting/stopping attack, normal operation. Negative for disruption, stolen data…

Identifying Attackers in a Mobile Social Network

Identifying Attackers in a Social Network

- Mobile social Network
- Users are “nodes”
- Information is passed to some nodes through other nodes which are connected to the server

Identifying Attackers in a Social Network

- Model:
  - Two types of nodes, benign (user) or malicious (attacker)
  - “Server” connects with nodes
  - Actions for server: Nothing, Packet, surveillance
  - Actions for node: Forward, Ignore, Damage
  - If server does no surveillance, then malicious nodes can infiltrate network
  - If server surveils everyone, the service for everyone suffers
- Goal is to find balance
  - “Therefore, the most compelling network security problem is to correctly define a proper operation where both types of clients are considered, and efficient defence strategies are designed with the purpose of preventing malicious activities and providing good quality services to benign nodes”

The Game From the Server

Connect with a node, then I……

1. **Do Nothing**
   Nobody wins - but safe I guess?

2. **Send node a Packet**
   Normal operation - good if node is benign, bad if node is malicious

3. **Set up surveillance on node**
   Try to catch malicious node - good if node is malicious, bad if node is benign

The Game From the node

Connect with server, then I……

1. **Do Nothing**
   Nobody wins - Discard packet if received

2. **Forward Packet**
   Normal operation - good for benign node, bad for malicious node

3. **Damage Packet**
   Do evil things - always bad for benign node, for malicious node, good if packet, bad if surveillance

		Player 2		
		Forward	**Ignore**	**Damage**
Player 1	**Nothing**	$0, -1$	$0, 0$	$-1, -\infty$
	Packet	$1, 1$	$-1, 0$	$-2, -\infty$
	Surveillance	$-3, -2$	$-3, 0$	$2, -\infty$

TABLE I
NORMAL-FORM (MATRIX) OF THE GAME WITH A BENIGN PLAYER 2

		Player 2		
		Forward	**Ignore**	**Damage**
Player 1	**Nothing**	$0, -1$	$0, 0$	$-1, 1$
	Packet	$1, -1$	$-1, 0$	$-2, 3$
	Surveillance	$-3, -2$	$-3, 0$	$2, -3$

TABLE II
NORMAL-FORM (MATRIX) OF THE GAME WITH MALICIOUS PLAYER 2

Dominated Strategy: Strategy or move in game theory where the payoff can always be better by doing something else

For Benign node: Damage is dominated by ignore

For Malicious node: Forward is dominated by ignore

Findings

- “The best strategy for the server would not be to always identify malicious clients, but rather to force them to strategically play some less harmful strategies.”
- Malicious nodes want to avoid being caught by invisible surveillance…. Best strategy would be to sometimes cooperate with network

		Player 2			
		IF	**II**	**DF**	**DI**
Player 1	**N**	0, p-1	0, 0	-p, 2p-1	-p,p
	P	1-2p, 1-p	-1, 0	1-3p, 2p+1	-p-1, 3p
	S	-3, -2+2p	-3, 0	5p-3, -p-2	5p-3, -3p

TABLE III
NORMAL-FORM (MATRIX) OF THE BAYESIAN GAME

		Player 2	
		IF	**DI**
Player 1	**N**	0, 0	-p, p
	S	-3, 0	5p-3, -3p

TABLE V
SIMPLIFIED NORMAL-FORM (MATRIX) OF THE BAYESIAN GAME

Markov Game Model

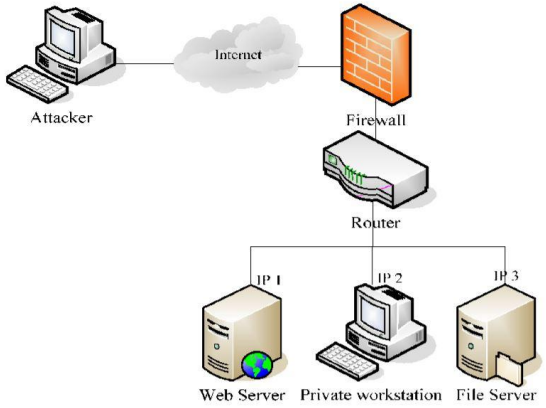
Markov Game Model

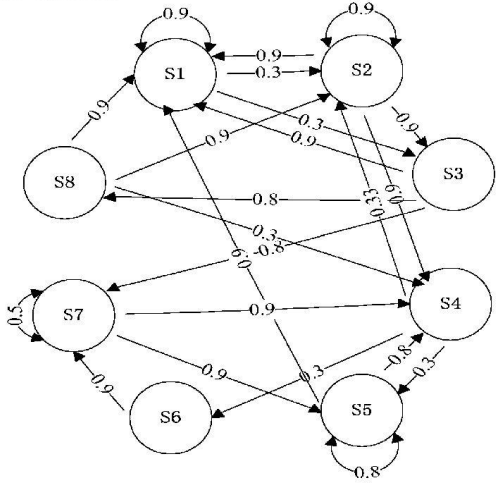
The Model:

- Set of states s
- Player chooses action based on actions available at state s
- At next step randomly move to s’
    - Based on probabilities from current state and action chosen
- Player gets reward based on move R(s, s’)
- State transition p’s calculated with case studies, stats, simulations, and knowledge engineering
- Use non-linear program to find stationary equilibrium

Improvements over peer research:

- State model works well in describing a real system
- Uses randomness (attackers don’t always make predictable moves - not complete info)





Example used for analysis of Markov Game Model

Network state	Attack strategies	Defense strategies
Normal state (s_1)	π_1^a ={Attack http, Attack ftp, Φ}	π_1^d ={Φ, Φ, Φ}
Http attacked state (s_2)	π_2^a ={Continue attacking, Φ, Φ}	π_2^d ={Remove sniffer detector, Φ, Φ}
Website defaced state (s_3)	π_3^a ={Deface website, Install sniffer, Φ}	π_3^d ={Remove compromised account, Install sniffer detector, Φ}
Ftp attacked state (s_4)	π_4^a ={Run DOS virus, Φ, Φ}	π_4^d ={ Remove compromised account, Restart Ftp server, Φ}
Fileserver hacked state (s_5)	π_5^a ={Crack file server root password, Φ, Φ}	π_5^d ={Remove virus and compromised account, Φ, Φ}
Web server data stolen state (s_6)	π_6^a ={Crack web server password, Φ, Φ}	π_6^d ={Remove sniffer detector, Install sniffer detector, Φ}
Workstation hacked state (s_7)	π_7^a ={Crack workstation root password, Φ, Φ}	π_7^d ={Remove sniffer detector, Remove compromised account, Φ}
Workstation data stolen state (s_8)	π_8^a ={shut down network, Φ, Φ}	π_8^d ={ Install sniffer detector, Remove compromised account, Φ}

The objective function:

$$\text{minimize } [v_1\text{-}(10a_1^1d_1^1+10a_1^1d_1^2+10a_1^1d_1^3+10a_1^2d_1^1+10a_1^2d_1^2+10a_1^2d_1^3)$$
$$\text{-}0.6(0.9v_1+0.33v_2+0.33v_3)]+[v_2\text{-}(20a_2^1d_2^1+10a_2^1d_2^2+10a_2^1d_2^3)$$
$$\text{-}0.6(0.9v_1+0.9v_2+0.9v_3+0.9v_4)]+[v_3\text{-}(90a_3^1d_3^1+50a_3^1d_3^2$$
$$+99a_3^1d_3^3+10a_3^2d_3^1+10a_3^2d_3^3-10a_3^3d_3^2)\text{-}0.6(0.9v_1+0.8v_7+$$
$$0.8v_8)]+[v_4\text{-}(30a_4^1d_4^1+30a_4^1d_4^2+30a_4^1d_4^3+50a_4^2d_4^1+50a_4^2d_4^2+$$
$$50a_4^2d_4^3+50a_4^3d_4^1+50a_4^3d_4^2+50a_4^3d_4^3)\text{-}0.6(0.33v_2+0.3v_5+$$
$$0.3v_7)]+[v_5\text{-}(30a_5^1d_5^1+30a_5^2d_5^1+30a_5^3d_5^1)\text{-}0.6(0.9v_1+0.8v_4+$$
$$0.8v_5)]+[v_6\text{-}(999a_6^1d_6^1+999a_6^1d_6^2+999a_6^1d_6^2)\text{-}0.6(0.9v_6)]+[v_7\text{-}$$
$$30a_7^1d_7^1+60a_7^1d_7^2+60a_7^1d_7^3)\text{-}0.6(0.9v_4+0.9v_5+0.5v_7)]+[v_8\text{-}(30a_8^1d_8^1$$
$$+60a_8^1d_8^2+60a_8^1d_8^3)\text{-}0.6(0.9v_1+0.9v_2+0.3v_4)]$$

v - payoffs
a - attacker moves
d - defender moves

Constraint conditions:

$$v_1-(10d_1^1+10d_1^2+10d_1^3)-0.6\times0.33v_2\geq0$$
$$v_1-(10d_1^1+10d_1^2+10d_1^3)-0.6\times0.33v_3\geq0$$
$$v_2-20(d_2^1+10d_2^2+10d_2^3)-0.6(0.9v_3+0.9v_4)\geq0$$
$$v_2-0.6\times0.9v_1\geq0$$
$$v_3-(90d_3^1+50d_3^2+99d_3^3)-0.6\times0.8v_3\geq0$$
$$v_3-(-10d_3^2)-0.6\times0.9v_1\geq0$$
$$v_4-(30d_4^1+30d_4^2+30d_4^3)-0.6\times0.33v_2\geq0$$
$$v_4-(50d_4^1+50d_4^2+50d_4^3)-0.6\times0.3v_5\geq0$$
$$v_4-(50d_4^1+50d_4^2+50d_4^3)-0.6\times0.3v_7\geq0$$
$$v_5-30d_5^1\geq0$$
$$v_5-30d_5^1-0.6\times(0.9v_1+0.8v_4+0.8v_5)\geq0$$
$$v_6-(999d_6^1+999d_6^2+999d_6^3)-0.6\times0.9v_7\geq0$$
$$v_7-(30d_7^1+60d_7^2+60d_7^3)-0.6(0.9v_4+0.9v_5+0.5v_7)\geq0$$
$$v_8-(30d_8^1+60d_8^2+60d_8^3)-0.6\times0.3v_4\geq0$$
$$v_8-0.6\times0.9v_1\geq0$$
$$v_8-0.6\times0.9v_2\geq0$$
$$\sum_{i=1}^{3}a_k^i=1,\quad\sum_{j=1}^{3}d_k^j=1,\text{且}a_k^i\geq0,d_k^i\geq0$$

Drawbacks

Main Theme: Models are not sophisticated enough, or cannot scale to be so.

- A large bulk of early research focussed on perfect information games.
- Most thorough models would require immense computational power to complete, if they are even feasible at full scale.
- Most models assume state transition probabilities are fixed
- Most models assume state transition probabilities can be calculated from domain knowledge and past statistics

Conclusion

Game theoretic approaches are a promising way to deal with network security!

However, we still have work to do before they can be effectively deployed to stop attackers.

Sources

[1] A Survey of Game Theory as Applied to Network Security

[2] Analysis of Strategic Security Through Game Theory for Mobile Social Networks

[3] An Analyzing Method for Computer Network Security Based on the Markov Game Model

[4] Lots of Wikipedia