Moving Assets to the Cloud: A Game Theoretic Approach Based on Trust

Louai Maghrabi & Eckhard Pfluegel

Wireless Multimedia and Networking Research Group
Faculty of Science, Engineering & Computing
School of Computing & Information Systems
Kingston University

Cybersecurity 2015
8^{th} – 9^{th} June

Overview

Motivation

Research Contributions

The Game Theoretic Model

Theorem

Examples

Conclusion & Future Research Directions

Motivation

- Idea of cloud computing: IT services will be provided as nowadays water & electricity
- Organisations invest huge resources to protect IT infrastructures rather than assessing risks
- Risk Assessment frameworks such as OCTAVE, TARA, FAIR, STRIDE & NIST RMF are difficult to apply to a cloud-based environment.
- Threat and vulnerability analysis is often based on identification of critical assets. (Asset information might not be available)
- The analysis effectively needs the cooperation of the cloud provider. But we cannot assume that this cooperation can be established.

Research Contributions

- We design a game theoretic cloud-based model for assessing risks to critical assets.
- Establish first model depending on trust degree T a user has in the cloud provider
- This solves the issue with a vulnerability v (exploiting asset a on the user's system) *shifting* to the cloud (resulting in a shifted vulnerability $\bar{v}$)
- Focus on user-centric model

The Game Theoretic Model

- Game $G = \{U, A, S^u, S^a\}$
- Players:
  - User U
  - Attacker A
- Strategies
  - S^u: User's Strategy
    - s_c^u: Put user's asset on cloud
    - s_h^u: Keep user's asset on user's system
  - S^a: Attacker's Strategy
    - s_u^a: Attack asset on user's system
    - s_c^a: Attack asset on cloud

Assumptions on the Cloud

- Note: The cloud provider is excluded from the game as a player.
- External attacks are usually unsuccessful, but in the event they are successful, compensation will be given
- The frequency of internal attacks depends on a parameter T
- We interpret this as the trust degree in the cloud provider:
    - $T = 1$: fully trusted cloud provider
    - $0 < T < 1$: partially trusted
    - $T = 0$: complete lack of trust

Cost Functions

- $C^u_{damage(v)}$ & $C^u_{damage(\bar{v})}$: user's damage from an attack on the asset through a vulnerability
- C^u_{fee}: cloud services subscription fees
- $C^u_{defend(v)}$: cost of user's defense
- $C^a_{attack(v)}$ & $C^a_{attack(\bar{v})}$: cost of accessing the asset through a vulnerability
- $C^a_{attack(\bar{v})} = (1 - T)^{-1} \cdot C^a_{attack(v)}$
- $C^u_{damage(\bar{v})} = (1 - T) \cdot C^u_{damage^*}$

Benefit Functions

- $B^{a}_{attack(v)}$: attacker's benefit from attacking user's a though v
- $B^{a}_{attack(\bar{v})}$: attacker's benefit from attacking user's a though $\bar{v}$
- $B^{a}_{attack(\bar{v})} = (1 - T) \cdot B^{a}_{attack(v)}$

Utility Matrix

	s^a_{user}	s^a_{cloud}
s^u_{cloud}	$-C^u_{fee} - C^u_{damage(\bar{v})}$, $-C^a_{attack(v)}$	$-C^u_{fee} - C^u_{damage(\bar{v})}$, $B^a_{attack(\bar{v})} - C^a_{attack(\bar{v})}$
$s^u_{in-house}$	$-C^u_{defend(v)} - C^u_{damage(v)}$, $B^a_{attack(v)} - C^a_{attack(v)}$	0, $-C^a_{attack(\bar{v})}$,

Substitution

- $C^a_{attack(\bar{v})} = (1 - T)^{-1} \cdot C^a_{attack(v)}$
- $C^u_{damage(\bar{v})} = (1 - T) \cdot C^u_{damage*}$
- $B^a_{attack(\bar{v})} = (1 - T) \cdot B^a_{attack(v)}$

	s^a_{user}	s^a_{cloud}
s^u_{cloud}	$-C^u_{fee} - (1-T) \cdot C^u_{damage*}$, $-C^a_{attack(v)}$	$-C^u_{fee} - (1 - T) \cdot C^u_{damage*}$, $(1-T) \cdot B^a_{attack(v)} - (1-T)^{-1} \cdot C^a_{attack(v)}$
$s^u_{in-house}$	$-C^u_{defend(v)} - C^u_{damage(v)}$, $B^a_{attack(v)} - C^a_{attack(v)}$	0, $-(1 - T)^{-1} \cdot C^a_{attack(v)}$,

Theorem

- If $T = 1$ and the following condition is satisfied:

$$C^u_{defend(v)} + C^u_{damage(v)} > C^u_{fee} \tag{1}$$

then the strategy $S = (s^u_c, s^a_u)$ is a pure Nash equilibrium for G.

- If $T = 0$ and the following condition is satisfied:

$$C^u_{damage^*} > C^u_{defend(v)} + C^u_{damage(v)} - C^u_{fee} \tag{2}$$

then the strategy $S = (s^u_h, s^a_u)$ is a pure Nash equilibrium for G.

Illustration for $T = 1$

$T = 1$	s^a_{user}	s^a_{cloud}
s^u_{cloud}	$-C^u_{fee}$, $-C^a_{attack(v)}$	$-C^u_{fee}$, $-\infty$
$s^u_{in-house}$	$-C^u_{defend(v)} - C^u_{damage(v)}$, $B^a_{attack(v)} - C^a_{attack(v)}$	0, $-\infty$,

If we assume condition (1), then we have a pure Nash equilibrium

Example

We assume some numerical values for the different cost and benefit functions to obtain the following table:

$T = 0.5$	s^a_{user}	s^a_{cloud}
s^u_{cloud}	$-35, -60$	$-35, -10$
$s^u_{in-house}$	$-50, 50$	$0, -100$

We then use GAMBIT to calculate the mixed Nash equilibrium and probabilities

- $P(s^u_h) = 0.25$
- $P(s^u_c) = 0.75$
- $P(s^a_u) = 0.7$
- $P(s^a_c) = 0.3$

Conclusion & Future Research Directions

- Devised the first user-centric model using trust degree as a parameter (To our knowledge!)
- Our model will be extended to
  - cover several or all assets in order to have a more comprehensive picture of the overall risks
  - be more realistic by adding more action and players

Thank you!