Sufficiently Secure Peer-to-Peer Networks

Rupert Gatti[1] Stephen Lewis[2] Andy Ozment[2]
Thierry Rayna[1] Andrei Serjantov[2]

[1]Faculty of Economics and Politics
University of Cambridge

[2]Computer Laboratory
University of Cambridge

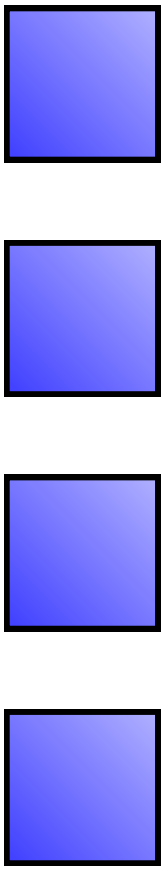
The Third Annual Workshop on
Economics and Information Security

UNIVERSITY OF CAMBRIDGE

Introduction

- Most threat models in computer security consider very powerful adversaries
- They lack a concept of how much a successful attack is worth to the attacker
- We consider a peer-to-peer censorship resistance system
- Can we estimate what levels of attack and defence we are likely to see in equilibrium?

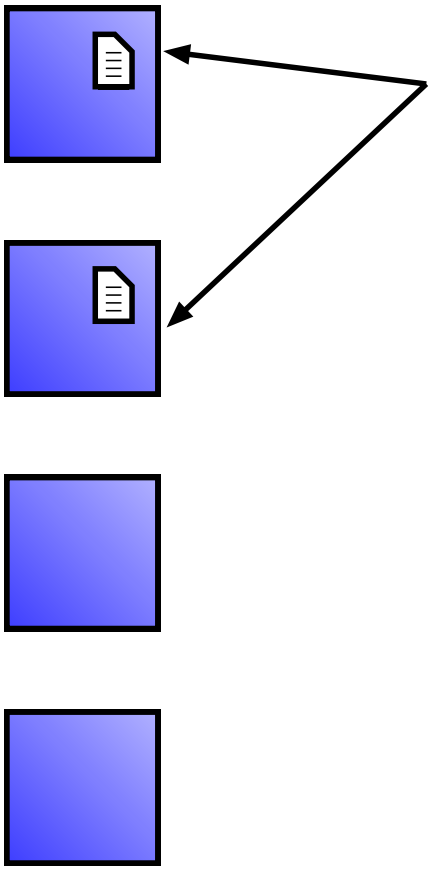
The Network



- Network of n nodes

$n = 4$

The Network

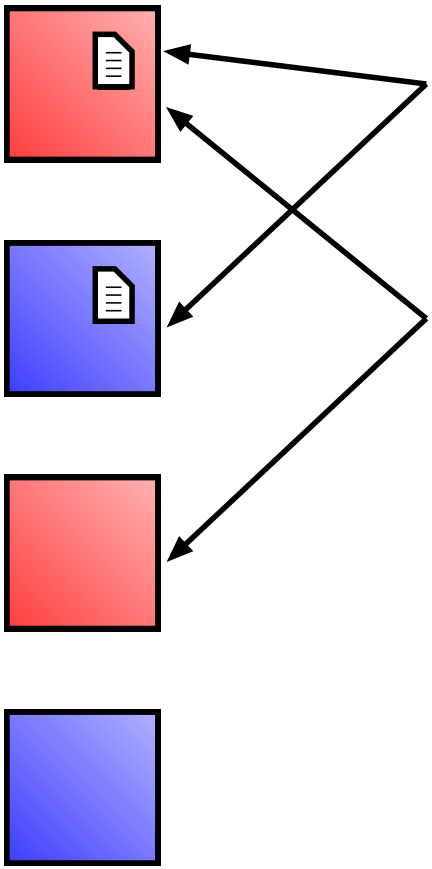


$n = 4$

$d = 2$

- Network of n nodes
- Documents published to d nodes

The Network



$n = 4$
$d = 2$
$x = 0.5$

- Network of n nodes
- Documents published to d nodes
- A proportion of nodes is corrupted: x

Utility Functions

- Publisher's goal: to ensure that at least one copy of his document resides in the network on a node that has not been corrupted
- Attacker's goal: to ensure that no copies of the document reside on nodes that have not been corrupted
- Model requires 'perfect search', and that the operation of the network is not affected by attack

Utility Functions

- Publisher's goal: to ensure that at least one copy of his document resides in the network on a node that has not been corrupted
- Attacker's goal: to ensure that no copies of the document reside on nodes that have not been corrupted
- Model requires 'perfect search', and that the operation of the network is not affected by attack

$$\begin{aligned} EU_p &= V_p[1 - x^d] - c_p d \\ EU_a &= V_a x^d - c_a n x \end{aligned}$$

Utility Functions

- Publisher's goal: to ensure that at least one copy of his document resides in the network on a node that has not been corrupted
- Attacker's goal: to ensure that no copies of the document reside on nodes that have not been corrupted
- Model requires 'perfect search', and that the operation of the network is not affected by attack

$$\begin{aligned} EU_p &= V_p[1 - x^d] - d \qquad \text{(normalized)} \\ EU_a &= V_a x^d - nx \end{aligned}$$

Attacker's Maximization Problem

The attacker needs to solve

$$\max_{0 \leqslant x \leqslant 1} \left[V_a x^d - nx \right]$$

Attacker's Maximization Problem

The attacker needs to solve

$$\max_{0 \leqslant x \leqslant 1} \left[V_a x^d - nx \right]$$

with first & second order conditions given by

$$\begin{aligned} \frac{\partial EU_a}{\partial x} &= dV_a x^{d-1} - n \\ \frac{\partial^2 EU_a}{\partial x^2} &= d(d-1)V_a x^{d-2} \end{aligned}$$

Attacker's Best Response

There is no interior solution in this case: the rational attacker will always attack either all of the network ($x = 1$) or none of it ($x = 0$).

Attacker's Best Response

There is no interior solution in this case: the rational attacker will always attack either all of the network ($x = 1$) or none of it ($x = 0$).

$$x = 0 \qquad \text{where } d = 0 \text{ or } V_a/n < 1$$
$$x = 1 \qquad \text{otherwise}$$

Publisher's Best Response

- We need only consider responses to $x = 0$ and $x = 1$

Publisher's Best Response

- We need only consider responses to $x = 0$ and $x = 1$
- If $x = 0$ (no attack), it is sufficient to publish a single copy of the document ($d = 1$)

Publisher's Best Response

- We need only consider responses to $x = 0$ and $x = 1$
- If $x = 0$ (no attack), it is sufficient to publish a single copy of the document ($d = 1$)
- If $x = 1$ (complete attack), there is no point in publishing, so set $d = 0$

Payoff Matrix for Attacker/Publisher Game

Attacker \ Publisher	P	$\bar{P}$
A	$V_a - n, -1$	$V_a - n, 0$
$\bar{A}$	$0, V_p - 1$	$V_a, 0$

UNIVERSITY OF CAMBRIDGE

Utility functions revisited

We now introduce an exponent α into the attacker's utility function, giving

$$\begin{aligned} EU_p &= V_p[1 - x^d] - d \\ EU_a &= V_a x^d - (nx)^\alpha \end{aligned}$$

Condition for Nash Equilibrium in Pure Strategies

- If $d > \alpha$, there is no Nash Equilibrium in pure strategies (second derivative of EU_a is always positive)
- If $d < \alpha$, the attacker's utility function has a maximum between $x = 0$ and $x = 1$, giving best response at $d = k$

$$x_k^* = \left(\frac{\alpha n^\alpha}{dV_a} \right)^{1/(k-\alpha)}$$

UNIVERSITY OF CAMBRIDGE

Condition for Nash Equilibrium in Pure Strategies (2)

- The publisher's utility function is at a maximum at $d = k$ if

$$\begin{aligned} EU_p(k-1) &< EU_p(k) \qquad \text{and} \\ EU_p(k+1) &< EU_p(k) \end{aligned}$$

- This gives the constraint on V_p

$$\frac{1}{x_k^{*k-1}(1-x)} < V_p < \frac{1}{x_k^{*k}(1-x)}$$

Example Solution

- With this constraint, we can now find an example where the equilibrium strategies of the attacker and the publisher are to attack part of the network, and publish to part of the network
- In a network with 1000 nodes and 2 copies of the publisher's document deployed, we set $\alpha = 3$ and $V_a = 3 \times 10^9$

Example Solution

- With this constraint, we can now find an example where the equilibrium strategies of the attacker and the publisher are to attack part of the network, and publish to part of the network
- In a network with 1000 nodes and 2 copies of the publisher's document deployed, we set $\alpha = 3$ and $V_a = 3 \times 10^9$
- The attacker's best response is to attack $2/3$ of the network, and thus any V_p between 4.5 and 6.75 will give an equilibrium in pure strategies

Mixed Strategies

- When there is no Nash equilibrium in pure strategies, we might still be able to find one in mixed strategies

  ▸ Payoff matrix

- λ_p is the probability of the publisher publishing one copy of his document
- λ_a is the probability of the attacker attacking and corrupting all the nodes

$$\lambda_a = \frac{V_p - 1}{V_p} \qquad \lambda_p = \frac{n^\alpha}{V_a}$$

Analysis

- 'Security' of the network depends on both its size (n), and the payoff the the attacker gets from successful censorship (V_a)
- Effective censorship is harder on larger networks: it is only worthwhile if the utility derived from successful censorship is large
- Uncontroversial content is still safe on small networks!

Analysis

- 'Security' of the network depends on both its size (n), and the payoff the the attacker gets from successful censorship (V_a)
- Effective censorship is harder on larger networks: it is only worthwhile if the utility derived from successful censorship is large
- Uncontroversial content is still safe on small networks!
- Attack cost that is linear in the number of nodes attacked gives 'all-or-nothing' solution – mixed strategies?
- Non-linear costs give a more interesting result: a network where the attacker and publisher are both expending some effort in their respective activities

Further Work

- More advanced model of search: can we find an equilibrium with three agents (publisher, censor and retriever)?
- Fragile networks: what if the attack impairs connectivity within the network?
- What will the effect of publishing documents as shares to different nodes be?
- How can we best model the situation where the attacker can add new nodes, as well as corrupt existing ones?
- Can the model be applied to peer-to-peer applications other than censorship resistance?

Conclusions

- Attackers will exhibit all-or-nothing behaviour within our simple model of a peer-to-peer network for censorship resistance
- Introducing non-linear costs for the attacker gives an equilibrium where both the censor and the publisher are expending some effort in their respective activities
- In the 'all-or-nothing' case, we have found a solution in mixed strategies

Conclusions

- Attackers will exhibit all-or-nothing behaviour within our simple model of a peer-to-peer network for censorship resistance
- Introducing non-linear costs for the attacker gives an equilibrium where both the censor and the publisher are expending some effort in their respective activities
- In the 'all-or-nothing' case, we have found a solution in mixed strategies
- Questions?

Multiple Publishers

- The new expected utility function of the attacker is:

$$EU_a = px^d - nx$$

- This is merely the expected value of a binomial distribution across the number of publishers whose documents are only stored on corrupt nodes
- The attacker's utility increases with the number of different documents he can suppress with the same effort