

# Colonel Blotto in the Phishing War

**Pern Hui Chia**

Centre for Quantifiable Quality of Service in Comm. Systems (Q2S), NTNU

**John Chuang**

School of Information, UC Berkeley

GameSec 2011, Nov 14-15, College Park, Maryland, USA

# Outline

- Background
  - Phishing
  - Colonel Blotto
- Modeling : Colonel Blotto Phishing game
- Analysis
- Implications to Anti-Phishing

# Background

# Phishing

- Annual Phishing losses?
  - \$15.6 billion in identity theft loss [FTC 2006]
  - \$3.2 billion in phishing loss [Gartner 2007]
  - \$61 million (with ~0.2% actual victim rate, \$200 median loss) [8]
- Characteristics:
  - ~30,000 phishing domains per 6-month [APWG]
  - Weak vs. strong phisher (e.g., Rock-Phish & Avalanche)
  - Different ways to host a phish (e.g., compromised servers, free-hosting services)
  - Can be hard to take down (e.g., Rock-Phish & Avalanche use fast-flux IP switching)
  - Not all phishes detected (information asymmetry)
- Q: What is the optimal strategy of a phisher?

Background:

# Colonel Blotto game

- 2-player constant-sum
- Allocation of finite resources in  $n$  battlefields
- Borel (1921)
- Borel and Ville (1938) : symmetric resources,  $n=3$
- Gross and Wagner (1950) : asymmetric resources, but solved  $n=2$  only  
.. [complex, lack of pure strategies] ..
- Roberson (2006) : characterization of unique equilibrium payoff

# Background: Colonel Blotto game

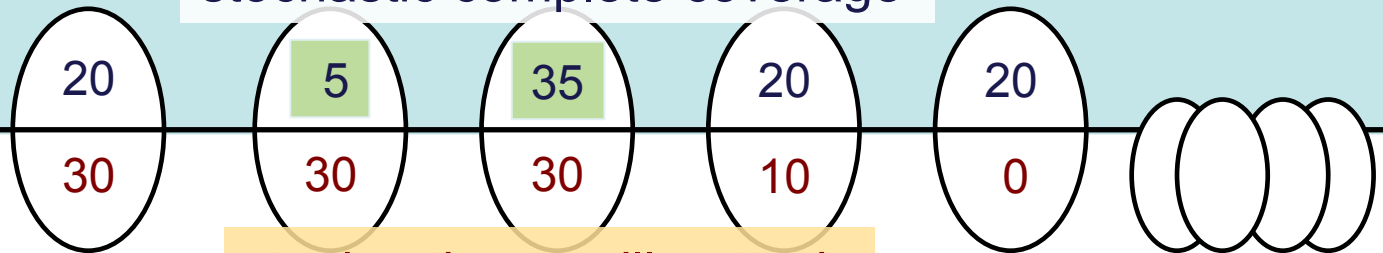
Application to Security?

Information asymmetry?

Colonel Blotto:

Limited resource = 100 soldiers

$n=5$



Attacker:

*Symmetrical resource = 100*

*Asymmetrical resource < 20 (trivial)*

*Asymmetrical resource > 20 (complex!)*

Kovenock et al. (2010):  
- endogenous dimensionality

Roberson (2006):  
- payoff w.r.t. resource asymmetry

# Modeling : Colonel Blotto Phishing (CBP)

# Colonel Blotto Phishing game

- Player: takedown company vs. phisher
- Battlefield: a phish
- Objective: maximize (minimize) fraction of phishes with more than a certain uptime
- Resource: infrastructure, manpower, time (finite) (use it or lose it) (defender has more resources)
- Cost: low: use a free-hosting service  
medium: register a new domain  
high: compromise a server

- Stage: (1) create – detect  
(2) resist – takedown
- Can phisher win in a detected battlefield?
  - No, if phisher's resource is much lower (total lock-down)
  - Yes, if phish survives a certain uptime
    - Not resolving phish URL at every access, or temporarily removing a phish [6]
    - Re-compromising a vulnerable server [7]
    - Fast-flux IP switching (e.g., by Rock-Phish & Avalanche)

# Phisher: How many new phishes to create?

S1

$$\begin{aligned} \max_{n_w} E(U_w | n_w) &= \frac{1}{n} E\left(\sum_{j \in \mathbb{J}_d} \pi_{w,j}\right) + \frac{(1 - P_d)n_w}{n} - cn_w \\ &= \underbrace{\frac{n_d}{n} E(\pi_w)}_{\text{detected phishes}} + \underbrace{\frac{(1 - P_d)n_w}{n}}_{\text{undetected phishes}} - \underbrace{cn_w}_{\text{cost}} \end{aligned}$$

S2

$$E(\pi_w) = \begin{cases} \frac{R_w}{2R_s} & \text{if } 1 \geq \frac{R_w}{R_s} \geq \frac{2}{n_d} \\ \frac{2}{n_d} - \frac{2R_s}{(n_d)^2 R_w} & \text{if } \frac{2}{n_d} \geq \frac{R_w}{R_s} \geq \frac{1}{n_d - 1} \\ 0 & \text{if } \frac{1}{n_d} \geq \frac{R_w}{R_s} \end{cases}$$

Roberson (2006)

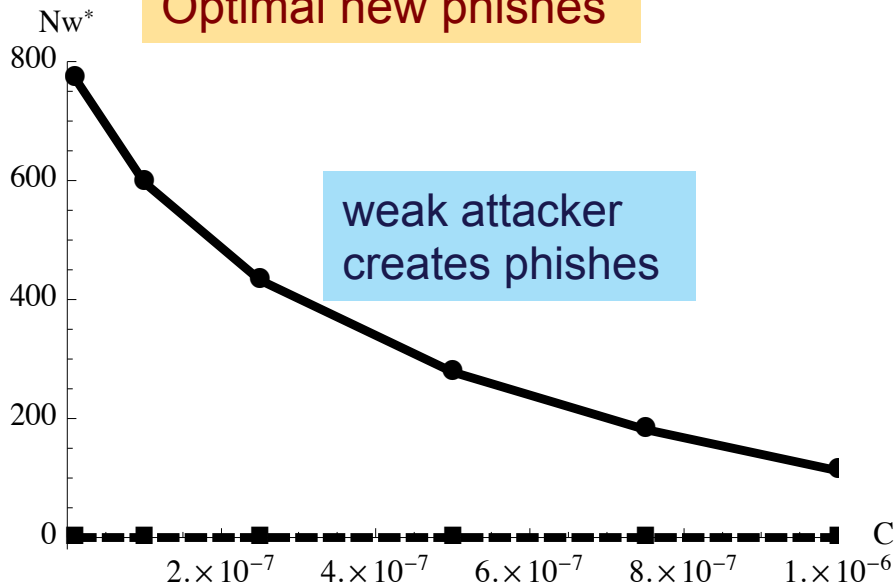
$$n_d = P_d n_w + n_0$$

$$n = n_w + n_0$$

# Analysis Results

# Perfect Detection (same settings as in [4])

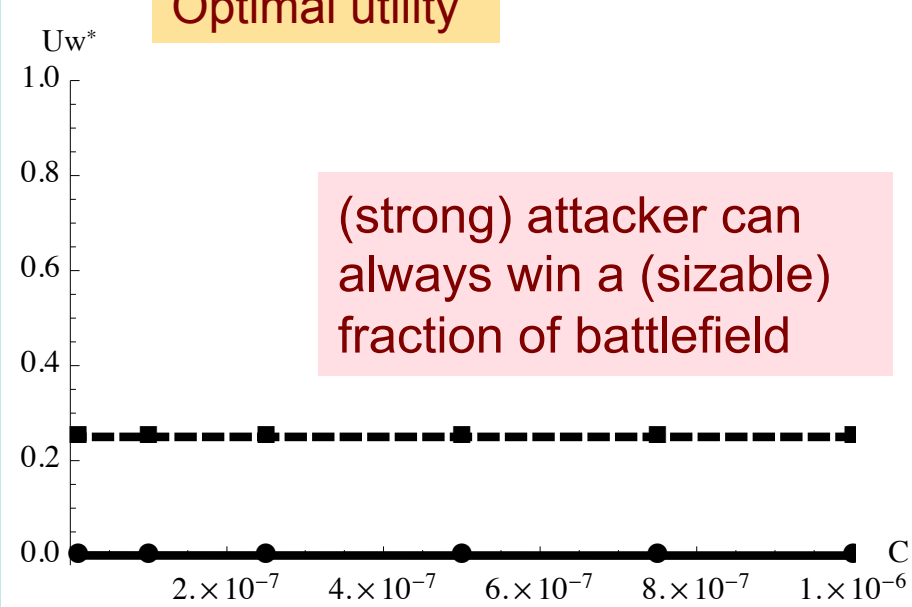
Optimal new phishes



weak attacker creates phishes

strong attacker creates no new phish

Optimal utility



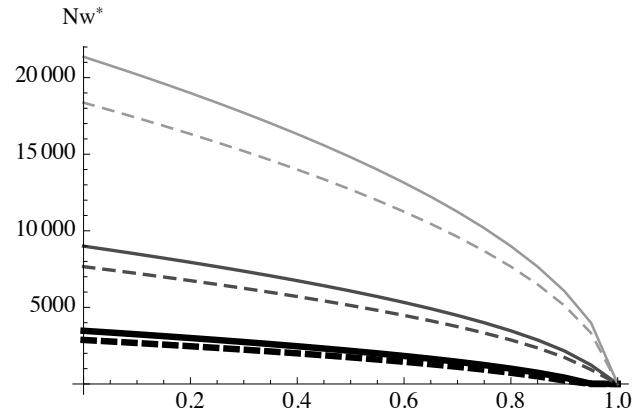
(strong) attacker can always win a (sizable) fraction of battlefield

weak attacker gets utility ≈ 0

- Resource asymmetry: strong attacker vs. defender = 1/2  
weak attacker vs. defender = 1/900

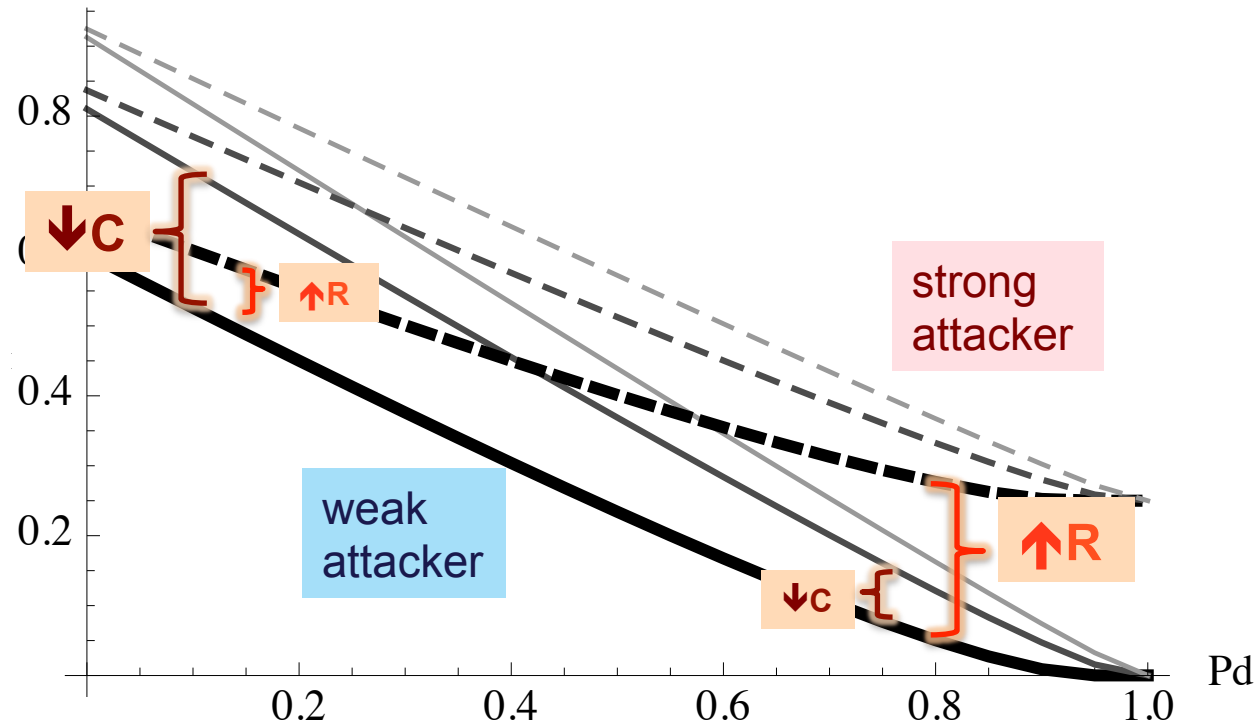
# Imperfect Detection (exogenous)

## Optimal new phishes



$Uw^*$

## Optimal utility

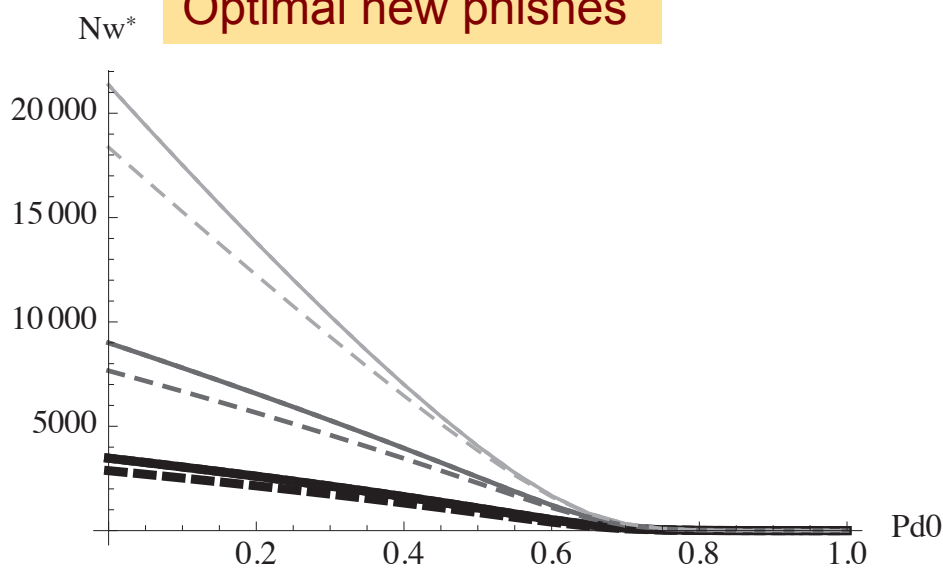


- Weak attacker creates more new phishes
- Weak attacker hurts more as  $Pd$  increases

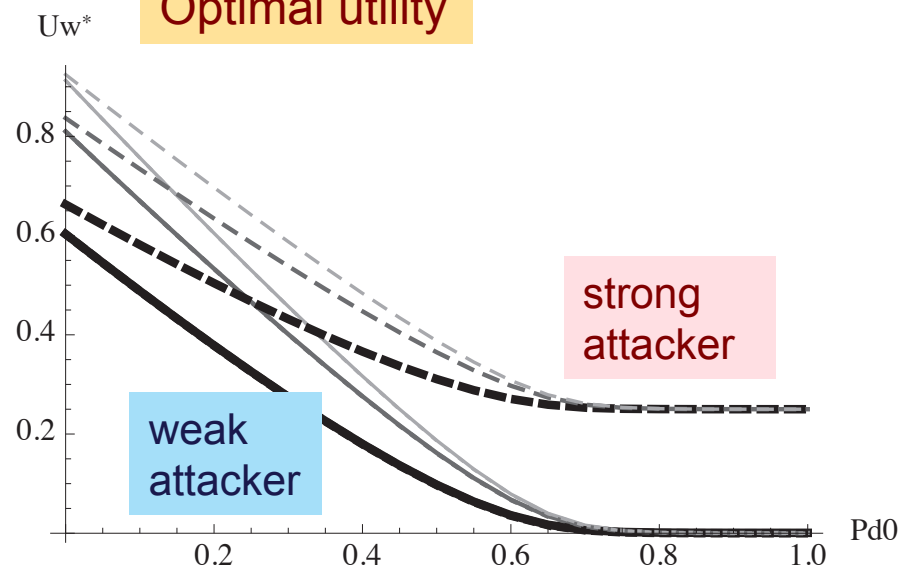
better off, if  $Pd \rightarrow 1$ : improve resources to resist takedown  
 if  $Pd \rightarrow 0$ : lower cost to create more phishes

# Imperfect Detection (endogenous)

### Optimal new phishes



### Optimal utility



- If new phishes increase detection rate
  - Registrars look for suspicious domain registration pattern [6]
  - ‘Rock Phish’ and ‘Avalanche’ phishes hosted on same domain [APWG]
- Less phishes and utility

# Discussion & Summary

# Implications to Anti-Phishing Industry

- Increasing cost of a phish
  - Affect a weak attacker more
  - But can use stolen credit cards, or ‘easy’ domains (e.g., .tk, co.cc) [6]
  - 80% attacks used compromised servers [6,7]
- Improving detection rate
  - Concerns for sharing among takedown companies
  - User reporting (not necessarily requiring user evaluation) can be helpful
- Empirical estimation & prioritizing
  - $P_d \rightarrow 0$ : make phishing cost higher
  - $P_d \rightarrow 1$ : disrupt resources (e.g., access to botnet, underground market)

# Summary

- Colonel Blotto Phishing (CBP)
  - Resource asymmetry
  - Information asymmetry
  - Endogenous dimensionality
- Applicability to web security problems
  - Two-step detect & takedown process
- Extensions
  - Competition between phishers -- Tragedy of the Commons? [8]

# Reference

1. E. Borel. La theorie du jeu les equations integrales a noyau symetrique. Comptes Rendus de l'Academie des Sciences, 173:1304–1308, 1921.
2. E. Borel and J. Ville. Application de la theorie des probabilities aux jeux de hasard. Paris: Gauthier-Villars 1938.
3. O. A. Gross and R. A. Wagner. A continuous colonel blotto game. RAND Corporation RM–408, 1950.
4. B. Roberson. The colonel blotto game. Economic Theory, 29(1):1–24, Sept. 2006.
5. D. Kovenock, M. J. Mauboussin, and B. Roberson. Asymmetric conflicts with endogenous dimensionality. Purdue University Economics Working Papers 1259, Dec. 2010.
6. APWG. Global phishing survey: Trends and domain name use in 2H2010.
7. T. Moore and R. Clayton. Evil searching: Compromise and recompromise of internet hosts for phishing. In *FC* 2009.
8. C. Herley and D. Florencio. A profitless endeavor: phishing as tragedy of the commons. In *NSPW* 2008.

Thank you. Questions?

Pern Hui Chia

[chia@q2s.ntnu.no](mailto:chia@q2s.ntnu.no)

John Chuang

[chuang@ischool.berkeley.edu](mailto:chuang@ischool.berkeley.edu)