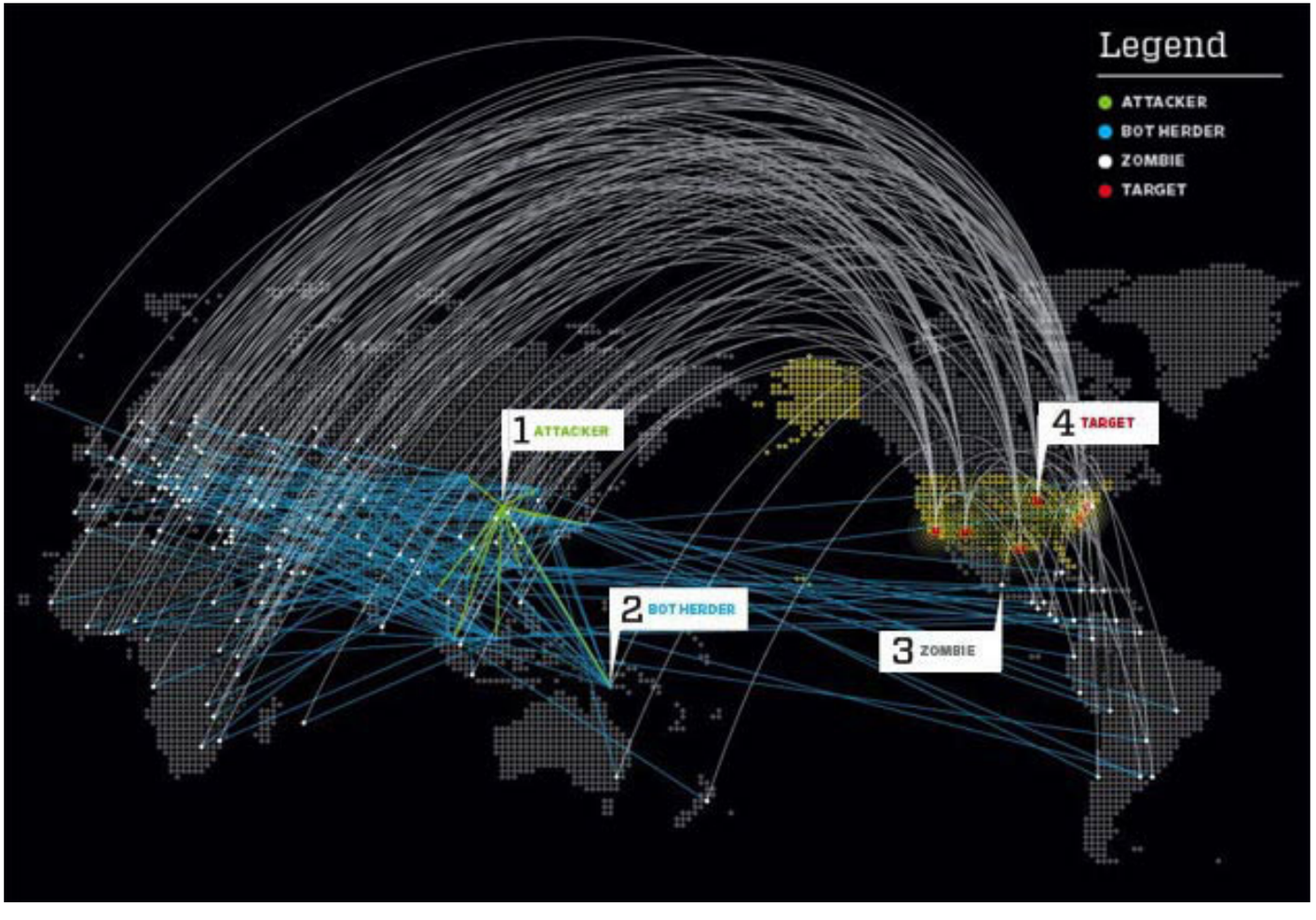
Distributed attacks as security games

Neal Fultz

Background

- WEIS
- *System reliability and free riding*, Varian 2002
- *Secure or insure*, Grossklags, Christin, and Chuang 2008.

Viruses, Zombies and Bots (Oh My!)



Approach and Contribution

- Motivation: Understand decision making in the context of networks under distributed attacks.

- More realism, nuance
  - Strategic attackers
  - Loosely coupled networks
  - Repeated interaction

- Methods
  - Formal game theoretic analysis
  - Simulation
  - Model fitting

Modeling

- N defenders (Blue)
  - Parameters: b, c, L
  - Variables: e, s
- M attackers (Red)
  - Parameters: p_c, F, L
  - Variables: p_a, k
- Contribution function H_e

Modeling cont.

$$
\begin{aligned}
Blue &= -(1-(1-p_a)^m)L(1-H_e)(1-s_i) - be_i - cs_i \\
Red &= \sum_{1}^{k} p_a L(1-H_e) - (1-(1-p_c)^k)F
\end{aligned}
$$

One on One

Results

- Deterrence: If $p_c F > L$, $(p_a, k) = (0, 0)$
- Passivity: If $b > L$, $(e, s) = (0, s^*)$
- Bounded Attack: Otherwise, $(p_a, k) = (b/L, 1)$

1 vs N: Tightly Coupled Networks

- Total Effort
  - $H_e = \frac{1}{N} \sum_{i=1}^{N} e_i$
  - Boundary: Nb/L
- Best Shot
  - $H_e = max(e)$
  - No upper boundary
- Weakest Link
  - $H_e = min(e)$
  - Boundary: b/L

1 vs N: Loosely Coupled Networks

- k-Weakest Targets
  - $H_e = \begin{cases} 1 & \text{if } e_i > e_{(k)} \\ 0 & \text{otherwise} \end{cases}$
  - $E(H_e) = \sum_{j=0}^{k} f_e^j (1 - f_e)^{N-1-j}$
  - No pure Nash $\longrightarrow$ No upper boundary
  - Mixed strategy:
    $f = \frac{b}{p_a L(N-k)\binom{N-1}{j}(\frac{1}{2})^{N-2}(1+2(2k-N)f_{e^*}(e-e^*))}$

1 vs N: Loosely Coupled Networks cont

- k-Weakest Targets with Mitigation
  - $H_e = \begin{cases} 1 & \text{if } e_i > e_{(k)} \\ e_i & \text{otherwise} \end{cases}$
  - $E(H_e) = (1 - \bar{e}) \sum_{j=0}^{k} f_e^j (1 - f_e)^{N-1-j}$
  - Upper boundary : choose k such that $Pr(k; N, e^*) < b/L$
  - Mixed strategy:
    $f = \frac{b}{p_a L} - .5^{N-1} \sum_{j=0}^{k-1} \binom{N-1}{j} + \binom{N-1}{k-1}(N-k).5^{N-2}(f_{e^*}(e - e^*)$
    all over $(1-e)\binom{N-1}{k-1}(N-k).5^{N-2}[1 + 2(2k-N)f_{e^*}(e-e^*)]$

M vs N

Additional constraint:

$$p_a = 1 - (1 - \text{Boundary})^{1/m}$$

Repeated Games

Trigger strategies generally lower the boundary by factor of N given sufficient discount factor δ.

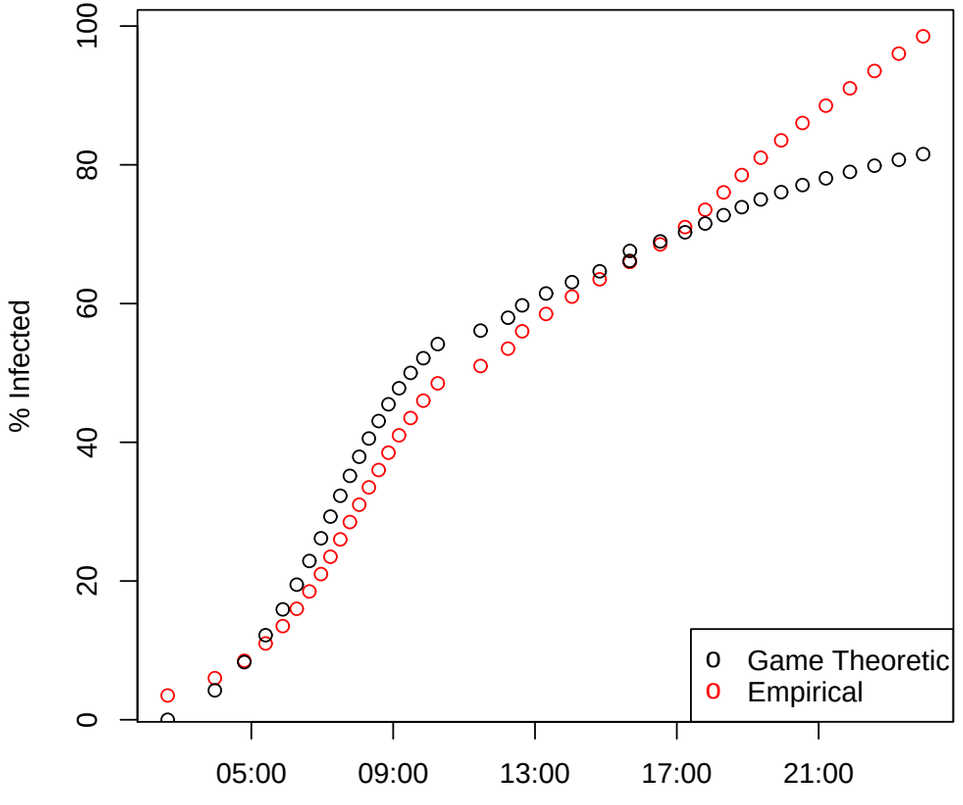
H_e	One Shot Ceiling	Repeated Ceiling
Total Effort	Nb/L	$\frac{bN}{L(1-\delta(N+1))}$
Weakest Link	b/L	b/L
Best Shot	1	$\frac{b(1-\delta)}{L(1-\delta^N)}$
Weakest Target	1	1
WT w/ Mitigation	***	***

Extensive-Form Games

- What about the contagious nature of malware?
  - Assume compromised machines become attackers
- Working in $lim_{N \to \infty}$, we find that there exists a tipping point where enough players have been compromised that N is small enough that attacking isn't profitable for all M.

$$m > \frac{ln(1 - p_a)}{ln(1 - \frac{p_c F}{NL})}$$

Model Fitting - Code Red



Results: b = \$50.88, $p_c = 0.48\%$, $\chi^2 = 47.4$, df = 38

Conclusions

- Policy
  - Real enforcement
  - Fines to fit the crime
- Design
  - Reduce the cost of protection
  - Minimize coupling

References

[1] J. Grossklags, N. Christin, and J. Chuang. Secure or insure? A game-theoretic analysis of information security games. In *Proceedings of the 2008 World Wide Web Conference (WWW'08)*, pages 209–218, Beijing, China, Apr. 2008.

[2] S. Schechter and M. Smith. How much security is enough to stop a thief? In *The Seventh International Financial Cryptography Conference (Gosier, Guadeloupe. January, 2003)*, 2003.

[3] H. Varian. System reliability and free riding. In L. Camp and S. Lewis, editors, *Economics of Information Security (Advances in Information Security, Volume 12)*, pages 1–15. Kluwer Academic Publishers, Dordrecht, The Netherlands, 2004.

Questions?