

Formally Specifying Design Goals of Worm Defense Strategies

Linda Briesemeister and Phillip A. Porras

`firstname.lastname@sri.com`

Computer Science Laboratory, SRI International

DETER Community Workshop

Jun 15–16, 2006



Outline

Worm Defense Evaluation — Current Practice and Our Aim

Understanding the Design Space of Worm Defenses

Design Goals of Quarantine-based Defense Techniques

- Weak Quarantine

- Quarantine with Local Benefit

- Quarantine with Strong Local Benefit

Summary: Applying Quarantine Definitions at Design Time



Worm Defense Evaluation

Current practice

- ▶ Centered on effect of defense on global infection growth
- ▶ Under assumption of certain worm propagation (e.g., random scanning, topological, hit-list, . . .)

Our aim

- ▶ Stating design goals in terms of impact on those who participate in defense
- ▶ Consider potential negative impact on participants
- ▶ Take into account future defense-aware worms

Understanding the Design Space of Worm Defenses

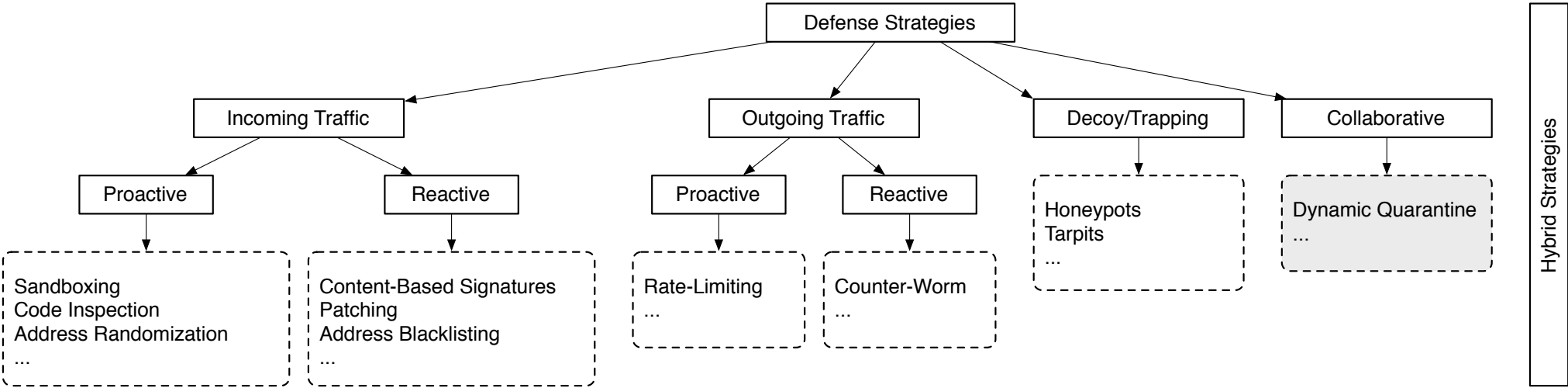


Figure: Design space of defense strategies (extended from Brumley et al. [2006])



Design Goals of Quarantine-based Defense Techniques

Preliminaries to understand following slides

- ▶ Consider participating population of N entities (LANs, organizations, hosts, etc.)
- ▶ Abstractly formulate notion of 2 states:
 - Infected Entity is infected with worm and aware of it
 - Quarantined Entity has potent filter in place or cut the cord
- ▶ Use Linear Temporal Logic (LTL) as formal language to express design goals
 - ▶ Global, sequential time
 - ▶ 2 temporal operators, \diamond (“eventually”) and \square (“henceforth”)

Outline Revisited

Worm Defense Evaluation — Current Practice and Our Aim

Understanding the Design Space of Worm Defenses

Design Goals of Quarantine-based Defense Techniques

- Weak Quarantine

- Quarantine with Local Benefit

- Quarantine with Strong Local Benefit

Summary: Applying Quarantine Definitions at Design Time

Weak Quarantine

Definition (“Weak Quarantine”)

Eventually every infected member of N is quarantined from N .
Formally,

$$\diamond(\forall j \in \{1..N\} : \text{Infected}[j] \Rightarrow \text{Quarantined}[j])$$

- ▶ But property is satisfied by strategy that is too slow and turns on quarantine too late, after all entities are infected!

Quarantine with Local Benefit

Definition (“Beneficial Quarantine”)

Eventually every infected member of N is quarantined from N and there exists an uninfected member within N . Formally,

$$\diamond((\forall j \in \{1..N\} : \text{Infected}[j] \Rightarrow \text{Quarantined}[j]) \\ \wedge (\exists k \in \{1..N\} : \neg \text{Infected}[k]))$$

- ▶ At least one is saved; one could make property stronger to define how many of N must be saved rather than just one.
- ▶ Note, algorithms using universal quarantine could satisfy this property, but what if quarantine comes at a cost?

Quarantine with Strong Local Benefit

Definition (“Strong Beneficial Quarantine”)

Eventually every infected member of N is quarantined from N and there exists an uninfected and not filtering member within N .

Formally,

$$\begin{aligned} & \diamond((\forall j \in \{1..N\} : \text{Infected}[j] \Rightarrow \text{Quarantined}[j]) \\ & \wedge (\exists k \in \{1..N\} : \neg \text{Infected}[k] \wedge \neg \text{Quarantined}[k])) \end{aligned}$$

- ▶ Now preventing unnecessary quarantine of saved member

Conclusion

Applying quarantine definitions at design time

- ▶ Thought-experiments and clarification of benefit and cost
- ▶ Perform model checking of properties against propagating worm model (not necessarily random scanning worm; could be non-deterministic)
- ▶ Inform simulation/emulation experiments; generate test cases

Open problems of formal methods in this context

- ▶ Stark abstraction needed (but may help bird's eye view)
- ▶ Moving from strong TRUE/FALSE to probabilistic models: more realism, but inching toward stochastic simulation
- ▶ Scalability to larger systems with more detail



Bibliography

David Brumley, Li-Hao Liu, Pongsin Poosankam, and Dawn Song. Design space and analysis of worm defense strategies. In *Proceedings of the 2006 ACM Symposium on Information, Computer, and Communication Security (ASIACCS 2006)*, March 2006. URL <http://www.cs.cmu.edu/~dbrumley/pubs/asiaccs06.pdf>.