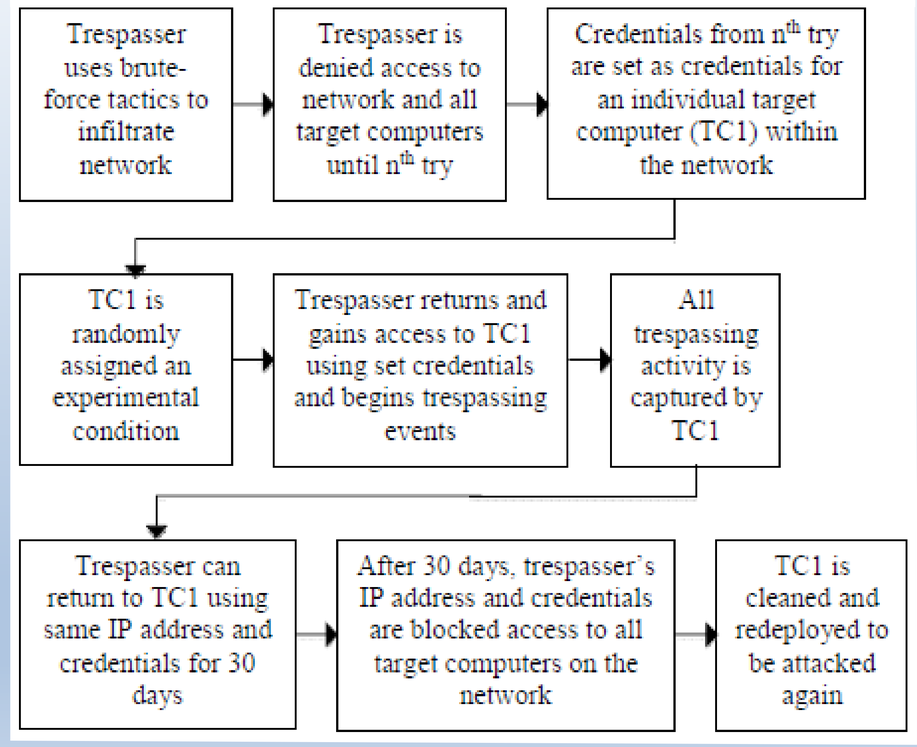
Is the Guardian Capable? A Routine Activity Theory Approach to Cyber Intrusion on Honeypot Systems

Michael Becker, BA, Michel Cukier, PhD, and David Maimon, PhD – University of Maryland

Theory and Research Questions

- Routine Activity Theory
  - Motivated Offenders
  - Suitable Targets
  - **Absence of Capable Guardians**
    - **RQ1**: Is there a difference in the number of sessions per attacker IP address across experimental conditions?
    - **RQ2**: In the presence of guardianship (root users), does the number of sessions per unique attacker IP decrease?
    - **RQ3**: Will the condition with both non administrative users and administrative users (C4) experience more attacks per attacker IP than conditions with only one administrative user (C2)?

Experimental Protocol*



Experimental Conditions

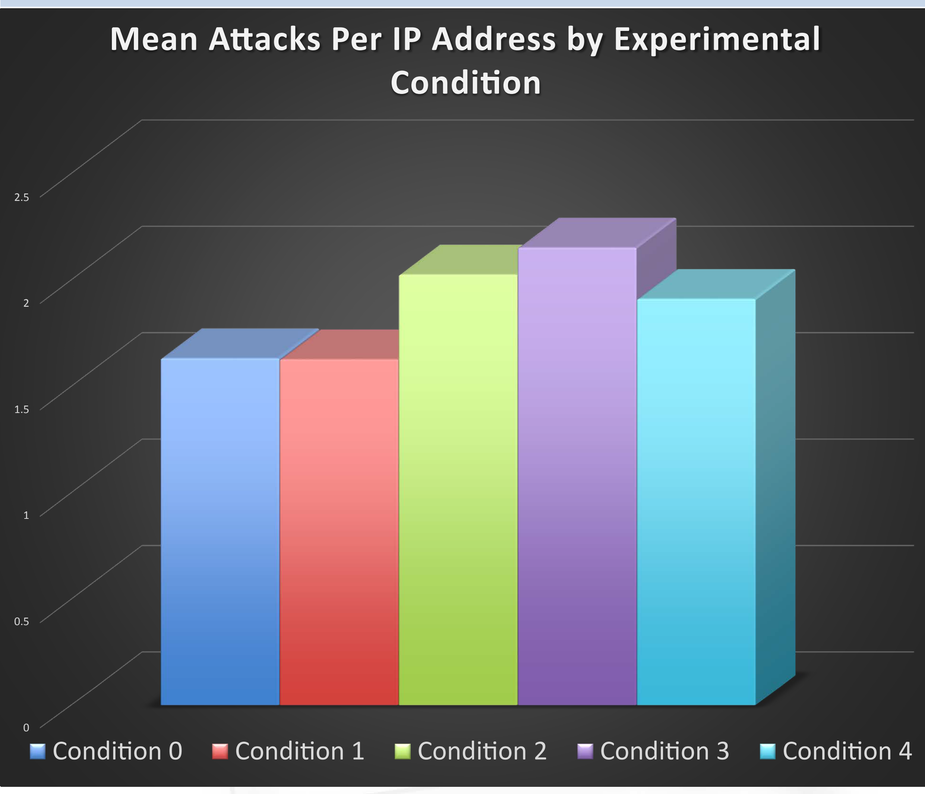
- Condition 0 (Control): No simulated users
- Condition 1: One non-root user
- Condition 2: One root user
- Condition 3: Ten non-root users
- Condition 4: Nine non-root users, one root user

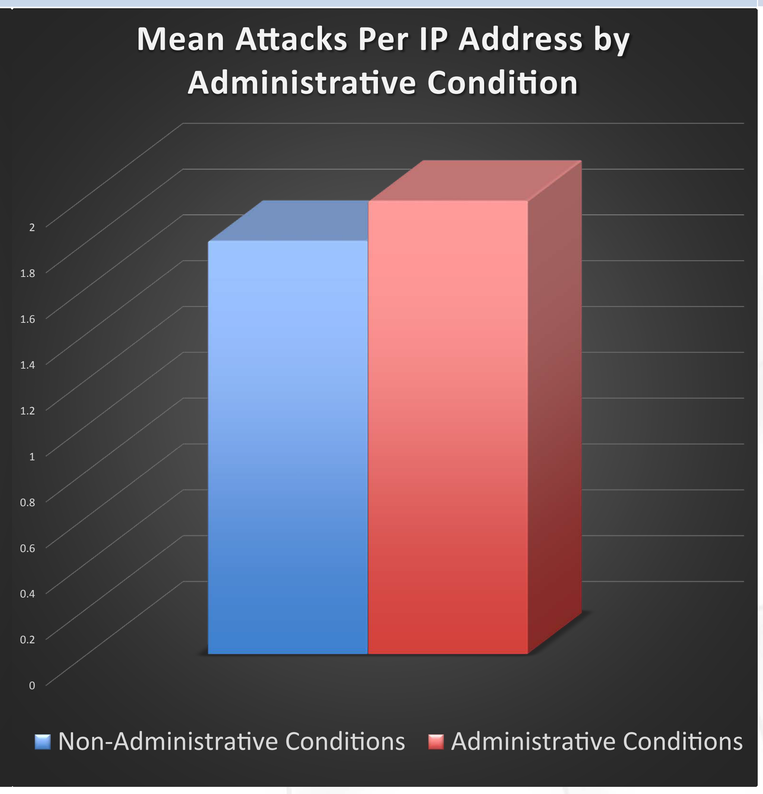
Data and Method

- Dependent Variable
  - Number of sessions per unique attacker IP address.
- Independent Variables
  - **RQ1**: Honeypot Condition (categorical)
  - **RQ2**: Administrative Condition (binary)
  - **RQ3**: Honeypot Condition (comparison between C4 and C2)
- Method
  - Pairwise mean comparison of conditions and sets of conditions using post-hoc Tukey tests to account for inflated probability of type 1 error.

Descriptive Statistics

Honeypot Condition	Sessions per Attacker IP		
	Mean	Median	Std. Dev.
Full Sample	1.839	1.333	1.324
Control	1.633	1	1.294
Condition 1	1.628	1.200	1.142
Condition 2	2.026	1.500	1.635
Condition 3	2.153	1.583	1.426
Condition 4	1.912	1.718	0.983





Conclusions and Limitations

- Non-significant findings represent the potential absence of a "guardianship" effect by entirely passive root users.
- Further research exploring the role of what constitutes "capable" guardianship in cyber situations is needed.
- At minimum, network engineers and system administrators must consider the role of active security programs and software in preventing network intruders from returning to already vulnerable systems.

HoTSoS Symposium and Bootcamp
HOT TOPICS *in the* **SCIENCE OF SECURITY**
APRIL 4-5, 2017 | HANOVER, MARYLAND

*Figure adapted from Remrey (2016)