



U.S. ARMY
RDECOM

Characterizing Burstiness in Intrusion Detection

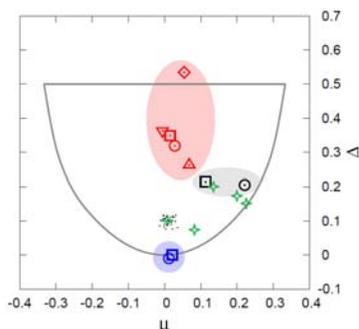


**S&T Campaign: Information Sciences
Cybersecurity**

Rich Harang, (301) 394-2444
richard.e.harang.civ@mail.mil

Research Objective

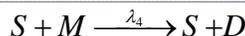
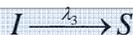
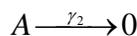
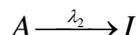
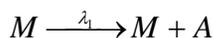
- Using real-world data, characterize, model, and predict the process of detection of network intrusion events; use these models to obtain actionable information about the state of the defended network



The intrusion detection process (green stars) falls between random processes (blue) and natural events (gray), but are distinct from human activity (red). Stochastic modeling approximately reproduces these characteristics (black dots; single model shown, n=30).

Challenges

- Quantifying burstiness and memory for use as a model selection target has been poorly explored
- The complexity of the malware lifecycle combined with limited observations (only detections times) poses a significant challenge when fitting models



$$\begin{aligned} dM_t &= -dN_{\lambda_4 S_t M_t} \\ dA_t &= dN_{\lambda_1 M_t} - dN_{\lambda_2 A_t} - dN_{\gamma_2 A_t} \\ dI_t &= dN_{\lambda_2 A_t} - dN_{\lambda_3 S_t} \\ dS_t &= -dN_{\lambda_2 A_t} \\ dD_t &= dN_{\lambda_4 S_t M_t} \end{aligned}$$

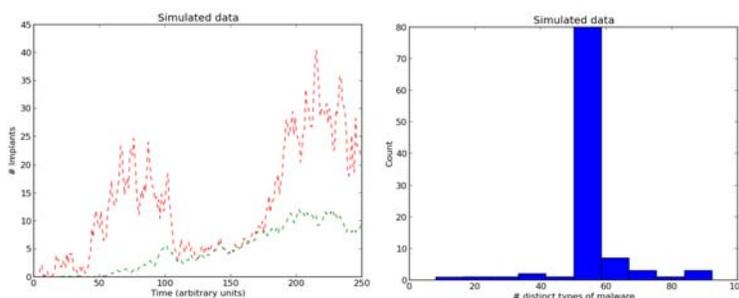
A simple generative stochastic model induces a system of stochastic differential equations that is straightforward to simulate, but extremely difficult to fit. Using various statistics of the simulated data as compared to the observed data we can nevertheless fit the model via approximate Bayesian methods.

ARL Facilities and Capabilities Available to Support Collaborative Research

- ARL Cyber Lab
- Network Science Research Lab (Q3 FY15)
- DOD HPC supercomputing resource center
- Real world incident data from a variety of categories of networks
- In-house expertise from CNDSP analysts

Recent Publications

- Harang, R. and Kott, A. 2013 "Modeling and forecasting of network incidents from partially observed data" MORS 81.2 Symposium (classified session)
 - Best Paper; Cyber Operations WG
- Harang, R. and Kott, A. 2014 "Burstiness of Intrusion Detection Process: Empirical Evidence, Characteristics and Possible Mechanisms" JSCoRE Vol. 1; Issue 1 (FOUO paper)
- Kott, A. and Harang, R. "Modeling of Burstiness and Latent Implants in the Intrusion Discovery Process" Submitted to JSCoRE



Posterior parameter estimates from fitted models allow for estimation of many quantities of interest, including latent malware implants on the network, and the number of distinct varieties of malware available. (Plots display fits to artificial data)

Complementary Expertise/ Facilities/ Capabilities Sought in Collaboration

- Publicly releasable data sets addressing the same topic
- Collaborations on alternate generative models and appropriate statistical measures for related problems