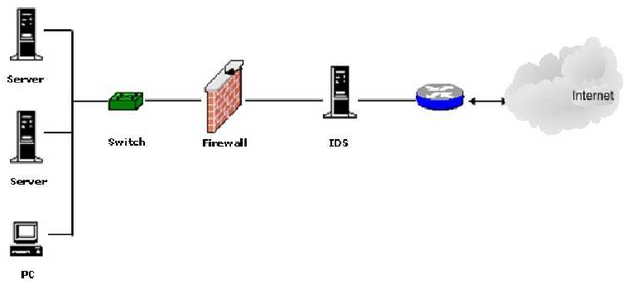
Characterization of Cyber Attack Actions through Variable Length Markov Models

Daniel S. Fava, Dr. Shanchieh Jay Yang (advisor)
Computer Engineering Department, Rochester Institute of Technology, RIT
{dsf7183,sjyeec}@rit.edu

Background

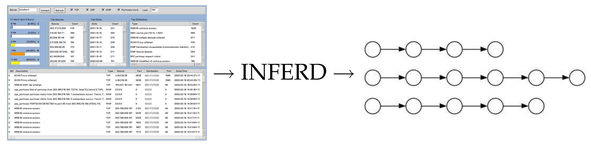
The increase in network bandwidth, the emergence of wireless technologies and the spread of the Internet throughout the world have created new forms of communication with effects on areas such as business, entertainment and education. This pervasion of computer networks into human activity has amplified the importance of cyber security.

Network security heavily relies on Intrusion Detection Systems (IDS), whose objective is to flag malicious activities.



Typical IDS setup

IDS alerts can be correlated into cyber attack tracks, which consist of sequences of alerts triggered by a single attacker. We study tracks of scripted attacks crafted by Skaion Corporation on behalf of the Air Force Research Laboratory. These attacks were correlated by Fusion Engine for Real-time Decision Making (INFERD).



From IDS alerts to attack tracks

Steps into alert correlation

- **Normalization and preprocessing**: creates a common set of fields across different alert levels.
- **Fusion**: combines duplicated alerts generated by the same attack action.
- **Thread reconstruction**: at a low level, this step combines several alerts belonging to a single attacker's actions.
- **Attack section reconstruction**: network- and host-based alerts are combined.
- **Focus recognition**: identifies Denial of Service (DoS) and port scannings by determining if a host is either the source or the target of many alerts.
- **Multistep correlation**: high level correlation in which scanning, intrusion, privilege escalation, etc are placed into a single attack track.

Objective

- Study attacks tracks and to enhance knowledge about attack behavior.
- Developed a Variable Length Markov Model (VLMM) for attack tracks.
- Build VLMM from from representative attack scenarios.
- Use model to infer future alerts given an attacker's recent history of actions.
- Measure the model's performance.

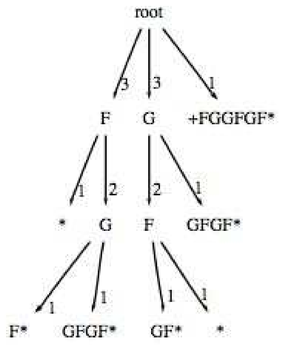
Theory

Attack tracks are translated into sequences $s_n = \{x_1, x_2, ..., x_n\}$, $x_i \in \Omega$. In an o order finite-context model, future events are dependent on o previous ones:

$$P^o(x_{n+1}|x_{n-o+1}, ..., x_n) = \frac{M[x_{n-o+1}, ..., x_n, x_{n+1}]}{M[x_{n-o+1}, ..., x_n]}$$

where $M[s]$ is the number of matches for the suffix s in the training set.

- Consider an attack sequence '$+FGGFGF*$'
- 'F' and 'G' correspond to Snort alerts 'WEB-IIS nsiislog.dll access' and 'WEB-MISC Invalid HTTP Version String.'
- '$+$' and '$*$' mark the start and the end of an attack sequence
- A suffix tree is the data structure chosen to hold finite-contexts
- Edges are weighed with the number of times the tree is traversed through that branch.
- Consider predicting the alert that follows '$s_a = \{+GF\}$'
- The longest match to s_a in the tree is 'GF' and it is followed by 'G' and '$*$' therefore $P^2\{G|GF\} = 1/2$ and $P^2\{*|GF\} = 1/2$
- $P^1\{G|F\} = 2/3$ and $P^1\{*|F\} = 1/3$
- $P^0\{F\} = 3/6$, $P^0\{G\} = 3/6$
- $P^{-1}\{F\} = P^{-1}\{F\} = 1/2$



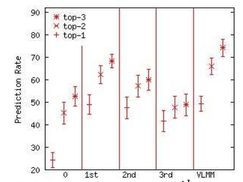
Note: The previous tree was built from a single attack sequence. However, in order for it to provide meaningful prediction, a suffix tree must be built from several representative attack sequences.

References

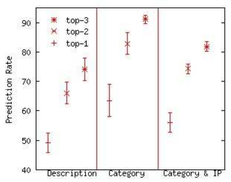
- Philippe Jacquet, Wojciech Szpankowski and Izydor Apostol. A universal predictor based on pattern matching. In *IEEE Transactions on Information Theory*, volume 48, pages 1462-1472, 2002.
- Daniel Fava, Jarred Holsopple, and Shanchieh Yang. Terrain and behavior modeling for projecting multistage cyber attacks. In *10th International Conference on Information Fusion*, Québec City, Canada, 2007.

Results

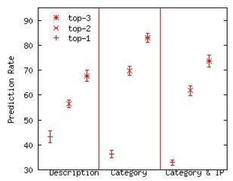
1. **VLMM versus 0^{th}, 1^{st}, 2^{nd}, and 3^{rd} order prediction**: a Variable Length Markov Model (VLMM) blends probabilities from multiple finite-context predictors of different orders. We show that the blended prediction is better than any individual finite-context predictor.
2. **Alert field choice and level of granularity**: alert fields reflect different aspects of an attack. For example, a VLMM can be created from Snort alert description or category fields. There are over 50 types of Snort descriptions that map into 9 categories. Choosing description over category impacts the level of granularity in the model.
3. **Repetition versus non-repetition**: the performance of VLMMs built from sequences that contain repetitions ($\exists\ i \mid x_i = x_{i+1}$) is contrasted with VLMMs created from sequences without repetition ($x_i \neq x_{i+1}\ \forall\ x_i$).



VLMM versus n^{th} order



No repetition



Repetition

Prediction rate is computed as the number of correct predictions over the total number of predictions.

4. **Frequency count and prediction rate**: events that have a higher frequency count in the data set tend to have higher prediction rates ('OpenSSL Worm traffic' is an exception).

Category	Description	Avg Pred Rate	Avg Freq
Trojan_Virus_Worm	OpenSSL Worm traffic	100.0%	5.5
Intrusion_Root	Invalid HTTP version string	94.8%	193.6
Intrusion_Other	Bare byte unicode encoding	91.2%	166.1
Recon_Scanning	ICMP L3retriever Ping	85.5%	61.8
Recon_Scanning	ICMP Ping nmap	78.1%	65.8
Intrusion_Root	NETBIOS SMB-DS IPC$ unicode share access	74.0%	45.3
Intrusion_Other	Oversize request-URI directory	71.5%	48.3

- Fredrik Valeur, Giovanni Vigna, Christopher Kruegel and Richard A. Kemmerer. A comprehensive approach to intrusion detection alert correlation. In *IEEE Transactions on Dependable and Secure Computing*, 01(3):146-169, 2004.
- Timothy C. Bell, John G. Cleary and Ian H. Witten. Text Compression. Prentice Hall, 1990.
- Ron Begleiter, Ran El-Yaniv and Golan Yona. On prediction using variable order markov models. In *Journal of Artificial Intelligence*, pages 385-421, 2004.

Acknowledgments: Thanks to CUBRC Corporation and the Air Force Research Laboratory for releasing the data set with which this research was conducted