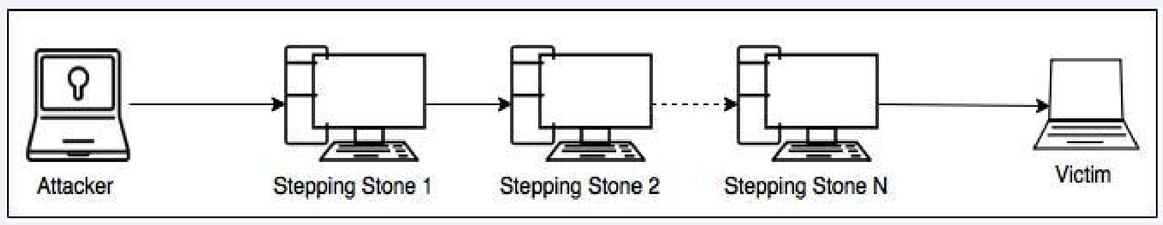
Detection of Stepping Stones in Software Defined Networks

Debopam Bhattacherjee, Andrei Gurtov, Tuomas Aura

Aalto University School of Science, Finland

Stepping Stones

Compromised hosts used as intermediate hops by hackers to hide identities.



Relevance in Today's Networks

Most of the papers are 10-15 years old.
Still relevant? Yes.

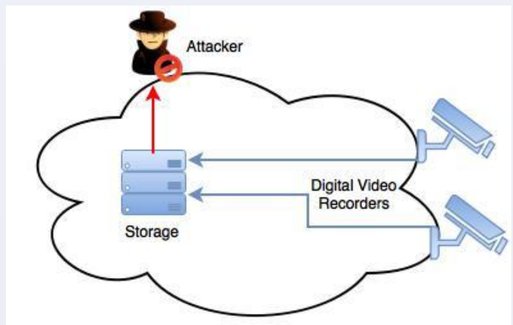
"APT", "Whistle-blower syndrome", "Hacktivism"

Panama Papers: "It was an email server attack"

05 APR 2016 10
Privacy, Data loss

The email hack includes 2.6TB of data, including 4.8 million email messages and 2.2 million PDFs

By Grant Gross FOLLOW
IDG News Service | Apr 5, 2016 9:25 AM PT



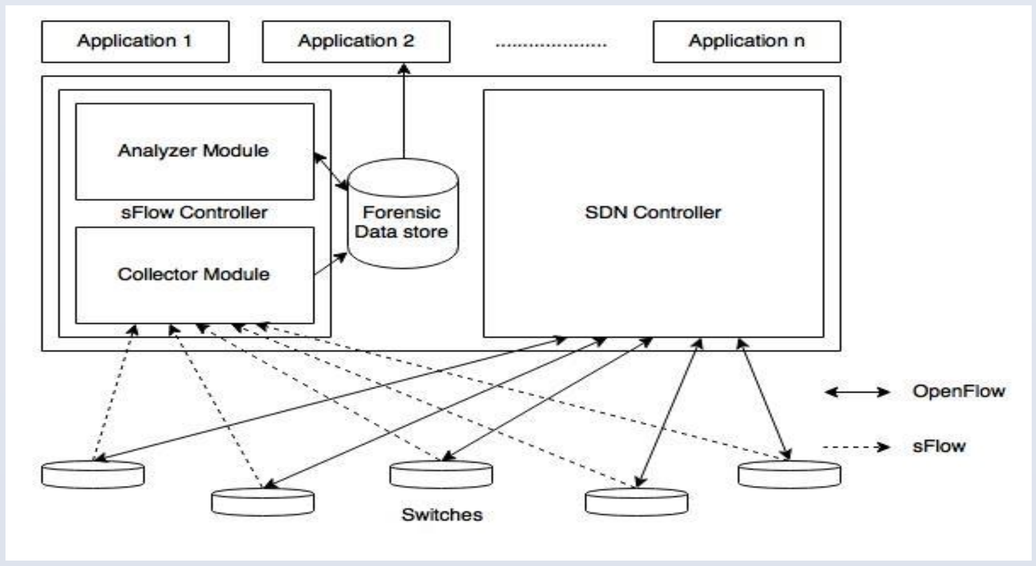
Detection Techniques Used

- **Transmission Characteristic-based Detection** [1]: Timing and packet-size based. Based on correlating ON and OFF periods generated by interactive traffic or traffic showing similar pattern.
  Correlated ON/OFF periods: Differ by $\leq \delta$ ms
  2 connections are correlated if:

$$\frac{OFF_{1,2}}{min(OFF_1, OFF_2)} \geq \gamma$$

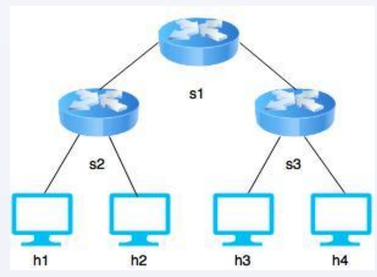
- **Anomaly-based Jitter and Chaff Detection Techniques** [2]:
  - Response-time based: Detects jitter
  - Edit-distance based: Detects chaff
  - Causality based: Detects Chaff

SDN-based Architecture for Detection

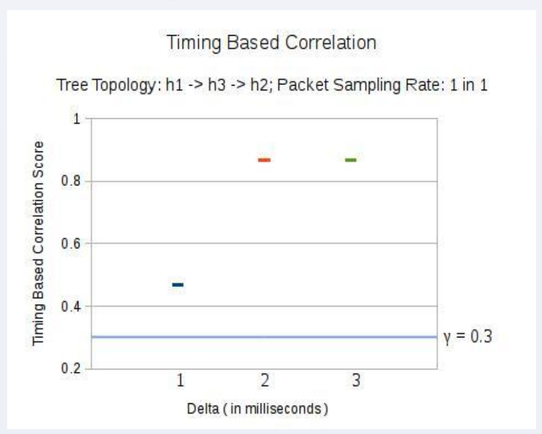


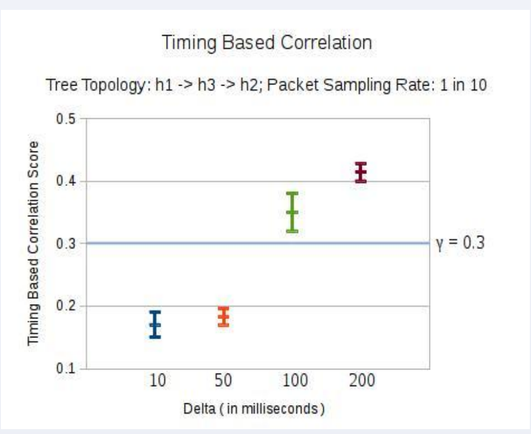
- **sFlow for network monitoring**: Packet sampling and immediate header information forwarding; Polling mechanism; Reduction in performance overhead compared to NetFlow/IPFIX; No flow cache

Important Results



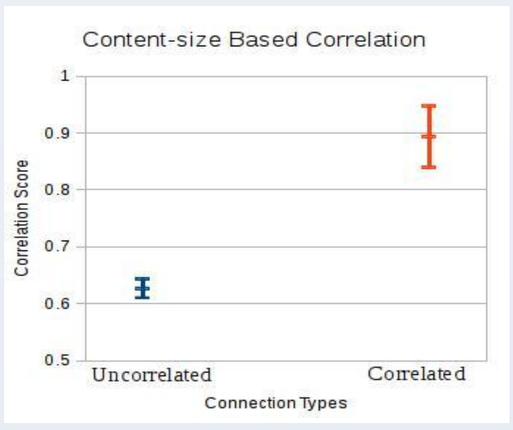
- Topologies tested on: Star, Tree, Linear. Here we present results for **tree topology.**
- Confidence level: 95%
- **Timing based correlation scores**





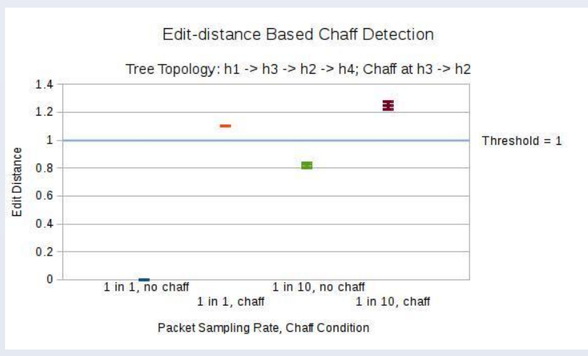
➔ Sampling disabled => Effective detection for very low δ
➔ Sampling enabled => Effective detection for $\delta \geq$100ms

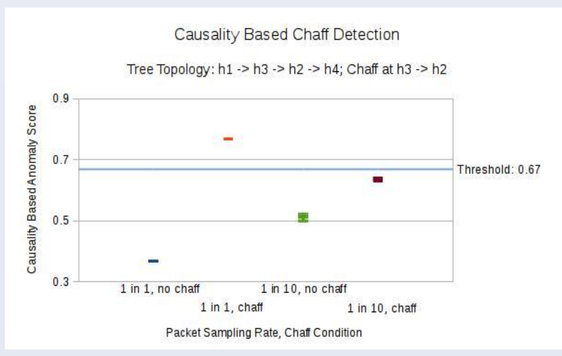
- **Content-size based correlation scores**



➔ Second-level check to reduce false positive rate
➔ Scores effectively differentiate positive and negative cases

- **Anomaly-based chaff detection**





➔ Edit-distance based chaff detection performs better than causality-based detection when sampling is enabled

Future Work

- De-anonymization: First link and last link traffic correlation on Tor-like networks.
- Incorporating sFlow polling mechanism
- Jitter detection
- Bot and botnet detection: Spatial and temporal communication analysis

References

[1] Zhang, Y., and Paxson, V. "Detecting stepping stones". In *Proceedings of the 9th Conference on USENIX Security Symposium - Volume 9 (Berkeley, CA, USA, 2000), SSYM'00, USENIX Association*, pp. 13.

[2] Di Crescenzo, G., Ghosh, A., Kampasi, A., Talpade, R., and Zhang, Y. "Detecting anomalies in active insider stepping stone attacks". *JoWUA 2 (2011)*, pp. 103-120.

Acknowledgment

The work has been done within the scope of the **CyberTrust SHOK** project funded by **DIGILE.**