TOWARDS EFFECTIVE SECURITY MONITORING FOR IOT

Siraj A. Shaikh

Founder & Chief Scientific Officer

CyberOwl

siraj.shaikh@cyberowl.io

Cybersecurity Policy Ideas for a New Presidency

Declarative Deterrence

" 'Privatized' active defense is an extraordinarily risky place to be. Others would benefit more than we would from a world where the shackles are off. The United States, in contrast, would benefit from a norm that 'states are responsible for attacks launched from their territory'.

Making a declarative public statement has the potential to bolster deterrence, broadening the range of punishments against which adversaries would have to calculate. "

CLTC, UC Berkeley, November 2016

Challenge of Attribution

Untangling Attribution

“ The most challenging set of attacks to investigate and deter are multi-stage attacks in which computer A penetrates computer B, which is used as a platform for penetrating computer C, which in turn attacks computer D.

Better attribution techniques will neither solve nor prevent such exploitations. ”

Clark and Landau, March 2011
HLS National Security Journal

Challenge of Attribution II

Untangling Attribution

“ Redesigning the network to accomplish robust attribution would not solve the most serious network-based cyber attacks and cyber exploitations being experienced today, which are **multi-stage** and **multi-jurisdictional**. ”

Clark and Landau, March 2011
HLS National Security Journal

Tallinn Manual

Section 2, Rule 6, Article 12

“ Consider a group in State A that assimilates computers located in State B into its botnet. The group uses the botnet to overload computer systems in State C based on instructions received from State D. The conduct is attributable under the law of State responsibility to State D.

Note that State A cannot be presumed responsible solely based on the fact that the group was located there, nor can it be presumed that State B bears responsibility for the groups acts merely because of the location of the bots on its territory. ”

Deception in the Cyberspace

Why Are Russian Hackers Posing as ISIS Propagandists?

" French and American investigators tracking the electronic footprints of the hackers found they led to a Russian hacker group known as APT28, which usually hack in favor of the Russian government and directs its efforts at NATO.

In fact, they found no electronic tracks leading back to ISIS. "

Helle Dale, Juy 24th, 2015
The Daily Signal

Noise!

Characteristics of internet background radiation

Increasing volumes of **non-productive traffic** in terms of

- continually growing scanning activity on public networks;
- backscatter traffic (response traffic from other scanning & attack activity); and
- traffic due to misconfigured hosts and administrative errors.

Most of such traffic is essentially defunct by the time it is visible on sensors.

Pang et al., 2004
Internet Measurement Conference

Security Alerts

“ The high volume of alerts requires a level of management that exceeds what most companies are realistically able to maintain. ”

Fireye, 2015
The Numbers Games: How Many Alerts is too Many to Handle?

Security Alerts II

Findings from the survey

- 37% of respondents indicated they face over 10k alerts/month;
- 30% say ‘low priority’ alerts take more than one day; and
- 60% say ‘moderate alert’ responses take between 6-12 hours.

Fireye, 2015
The Numbers Games: How Many Alerts is too Many to Handle?

The CyberOwl Vision

Shift from attribution to early warnings

- Protective monitoring of assets: Attribution is no longer the goal
- Focus on early warnings: serving to enhance and escalate sensing and control

Shift from signatures to indicators and symptoms

- Sensors sit beyond security control: Aim is to look for ‘unknown unknowns’
- Malicious behaviour always in variation: vital signs of system health have security value

The CyberOwl Vision II

Shift from prediction to judgement

- Alerts and indicators lead to estimations, which in turn invoke controls and policies
- Context is king: Security interpretation cannot be in isolation

Scalable environments by default

- Visibility across network, traffic and temporal spaces is key: stateful is not the approach
- Algorithmic underpinning for computational efficiency, to keep overheads low

Thank you