CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Using the Facts to Protect Enterprise Networks: CERT's NetSA Team

Key Message: Network defenders and business leaders can use NetSA measures and evidence to better protect their networks.

Executive Summary

The CERT Network Situational Awareness (NetSA) group develops engineering solutions and research approaches for analyzing broad network activity. The goal is to quantitatively characterize threats and targeted intruder activity. The process for providing network situational awareness includes knowing your network, knowing the Internet, and knowing how the two interact. NetSA methods and tools allow network defenders and decision makers to easily collect, analyze, and visualize what is going on on their networks so they can make more effective network security and protection investment decisions.

In this podcast, Tim Shimeall, a senior researcher with CERT, discusses practical approaches for determining what is happening on your networks and the networks to which you and your organization are connected.

PART 1: PROVIDING INSIGHT FOR NETWORK DEFENDERS AND DECISION MAKERS

NetSA Background and Scope

CERT's Network Situational Awareness Team (NetSA) has been in business since early 2001.

NetSA's research targets business leaders, decision makers, and network defenders to provide

- a quantitative understanding of network activity
- aids for making decisions as to how to defend networks and respond to potential threats
- methods and insight

NetSA's Analysis Approach

Due to the size and scope of the networks being analyzed (on the order of a CIDR/8 (Classless Inter-Domain Routing)), the team's research focuses on higher level abstractions of network activity (as contrasted with packet content). NetSA techniques have also been used on smaller networks.

One principle analysis abstraction is network flow data: aggregated header information without packet content. This information provides a record of all network communication, which can be more effectively analyzed to identify patterns and behaviors.

Intended Audience

The primary audience is

- network defenders including incident response staff
- those interested in traffic balancing, load balancing, network engineering, service inventory, and service control

The secondary audience is decision makers who manage members of the primary audience. NetSA analysis provides this audience with

- better education
- better ability to assess how well defensive measures are working
- better understanding of network operations

Network Situational Awareness: A Three Step Process

Step 1: know your network, both intended and accidental behavior

Step 2: know the Internet

- services you are providing
- services you are receiving
- threats that may affect you
- technology changes that may affect you

Step 3: know how these two fit and how internet behavior affects local network behavior

The scope of "know the Internet" is driven by your network points of presence (POPs) and those of your Internet Service Provider (ISP).

PART 2: ANALYZING AGGREGATED HEADERS, NETWORK FLOWS, AND COMMUNICATON PATTERNS

Analyzing Network Traffic

Analyzing aggregated header and network flow information involves examining

- services being provided and received
- communication partners
- communication patterns

Phishing is a good example.

- Detecting a phishing attack using message-by-message analysis is difficult.
- Phishing emails tend to be sent from very transient locations (different from normal email).
- Tracking normal email patterns and communication partners (called a locality set) and detecting transient variations can help in detecting phishing attempts and attacks.

Compacting Network Data

Network flow data can be captured and stored very efficiently. The characterization of gigabytes of traffic can be stored in 30 bytes of information.

Six months to one year of network flow data can be stored and analyzed online. This allows for precision in identifying trends and patterns.

The tool suite supporting this analysis is SiLK – System for Internet Level Knowledge.

Detecting Emerging Distributed Denial of Service Attacks

Spotting the ramp-up of a distributed denial of service (DDoS) attack involves

- having broad-scale knowledge of who you normally communicate with and the relative rate of communication
- noting the number of new hosts that are starting to communicate with your network, on unusual ports or using

unusual protocols
- detecting that the number of new hosts are rapidly passing the number of conventional hosts

If you can spot the ramp up early, you can work with your ISP to add rate throttling to preserve connectivity during the attack.

Detecting Excessive Bandwidth Consumption

NetSA analysis can aid in identifying

- excessive network bandwidth consumption by services and hosts and by ports and protocols
- an unusual amount of download activity
- excessive personal use in the workplace

PART 3: METHODS AND TOOLS; MAKING THE BUSINESS CASE

Visualizing Network Traffic Patterns

NetSA methods and tools can

- generate time series graphs of network utilization, broken out by common ports and protocols
- generate scatter graphs that identify the most common producers and consumers of network bandwidth
- detect scans and changes in scanning behavior
- determine what behavior is being exhibited by the network

Prioritizing Network Analysis

It is not unusual to spot weird behaviors; it doesn't make sense to analyze all of these. For example, misconfigured servers that emit bursts of behavior may not be a security problem but someone trying to flood out particular hosts likely is a problem worth analyzing.

Invest resources in analyzing traffic that affects mission-critical assets.

Additional Methods and Tools

RAVE (Retrospective Analysis and Visualization Engine) can be used to aid in visualizing network traffic.

Guidance is available for

- conducting a bandwidth study
- measuring activity across a specific set of ports or for a specific set of hosts

Evidence-Based Decision Making

NetSA's objective is to allow decision makers to make evidence-based decisions based on actual measures.

NetSA methods and tools allow CIOs to

- understand how their network is currently behaving as contrasted with how it is intended to behave
- rapidly recognize precursors to attacks such as DDoS and scans, independent of small details that are unique to a specific attack
- collect and store network traffic data economically

Resources

CERT NetSA web site

CERT NetSA tools web site