HomeTPS: Uncovering What is Happening in Home Networks

Kuai Xu, Feng Wang, and Michael Lee
Arizona State University

***Abstract*—The rapid growth of broadband connections and home networks has created new application opportunities such as video streaming and remote health care. However, managing and securing the increasingly complicated home networks has remained a serious challenge for most home users who have little technical expertise to manage their home networks and connected devices. Towards this end, we will demonstrate `HomeTPS`, a traffic profiling system for home networks that collects, analyzes and makes sense of home network traffic. The demonstration will show automatic traffic collection from programmable home routers, informative traffic summary reports and behavior profiles for Internet-capable home devices, and real-time discovery of anomalous traffic from Internet attackers or from compromised devices in home networks.**

I. Introduction

The last decade has witnessed the rapid growth of residential broadband connections and home networks that consist of a multitude of Internet-capable devices such as desktop machines, laptops, tablets, mobile phones, smart TVs, and gaming consoles [1]. The availability of home networks brings new application opportunities such as video streaming and remote health care, and has changed the landscape of Internet traffic. However, managing and securing the increasingly complicated home networks has remained a serious challenge for most home users, as they have little technical expertise or professional training to manage, secure and troubleshoot their home networks and connected devices [2], [3].

Many open-source tools or commercial products are available today to detect malwares such as viruses and worms or to filter known attacks through firewalls and intrusion detection systems. Unfortunately, there exist few simple and intuitive tools that could offer insights on traffic behaviors of home network devices. Towards this end, we develop a real-time behavior profiling system, `HomeTPS`, to collect, analyze and make sense of Internet traffic for Internet-capable devices in home networks. As illustrated in Figure 1, the profiling system, running from a separate server, captures traffic flows exported from programmable home routers [4] that connect home networks with the Internet via home gateways such as cable or DSL modems. Subsequently, the profiling system performs real-time traffic analysis of home network traffic. The primary objective of `HomeTPS` is to increase the visibility of network traffic, behavior patterns, and applications in home networks by uncovering *what is happening in home networks* [5].

In our demonstration we will show how `HomeTPS` provides a variety of functions to monitor and understand traffic summaries and communication patterns of connected devices through simple and intuitive interfaces for home users:

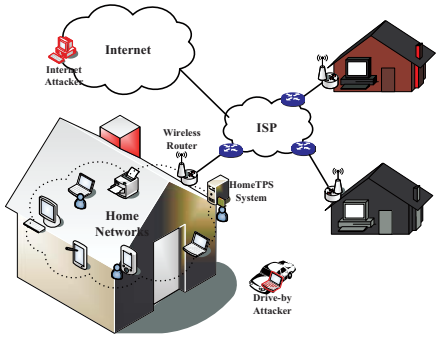

Fig. 1. Real-time traffic profiling system for home networks.

- Summarizing home network traffic: `HomeTPS` analyzes network traffic continuously exported from programmable home routers and generates succinct and meaningful summary reports that capture traffic volumes such network flows, packets, bytes for applications and home networks devices. `HomeTPS` also uses time series analysis to detect traffic deviations;
- Profiling network behaviors of home network devices: For each Internet-capable home device, `HomeTPS` makes sense of its communication patterns by exploring a variety of behavior features such as *who is talking with the device*, and *which applications does the device use*;
- Detecting anomalous traffic patterns: `HomeTPS` detects anomalous behavior patterns from both incoming and outgoing traffic, since the incoming traffic could include malicious traffic such as worms, viruses and scanning activities and the outgoing traffic could include anomalous malware or botnet traffic originating from compromised devices in home networks.

II. Traffic Profiling System

We have developed a prototype `HomeTPS` system and deployed in one real home network and one emulated home network in our computer networking research laboratory. Figure 2 illustrates the design of the profiling system that consists of three major system components: *traffic capture*, *behavior profiling*, and *event analysis*. Below we describe the primary functions of each component.

The *traffic capture* component in `HomeTPS` leverages programmable wireless home routers that is configured with OpenWrt, a Linux distribution for embedded devices [4]. Hence, `HomeTPS` is able to capture and analyze network flows exported from the routers. The continuous traffic flows are aggregated from IP packets and contain a number of important

978-1-4577-2071-0/12/$26.00 ©2012 IEEE

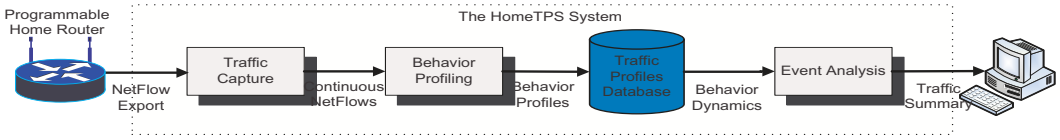

Fig. 2. The HomeTPS system design.

traffic features including the time-stamp, source IP address, destination IP address, source port number, destination port number, and protocol, packets and bytes.

To establish *behavior profiling* of Internet-capable home devices, HomeTPS captures behavior patterns of each device from five behavioral dimensions: 1) social, i.e., with whom does a home device communicate with; 2) functional, i.e., what role (e.g., client, server or peer) does the device play in the communication; 3) application, i.e., what application does the communication belong to; 4) volume, i.e., how much packets or bytes have been exchanged in the communication; and 5) temporal, i.e., is the communication consistent over time. Each of these dimensions captures the behavior of home devices from a unique perspective. Combined together they build comprehensive traffic profiles for these devices, and provide a broad picture of behavior patterns in home networks.

Finally the *event analysis* component focuses on analyzing abnormal traffic behavior in home networks. Specifically, HomeTPS further analyzes traffic summaries and behavior profiles of home devices via time-series analysis and correlation analysis. The results of event analysis will provide valuable input and feedback for home users to reconfigure home routers properly for improved security, e.g., adding firewall rules to filter unwanted traffic from the Internet.

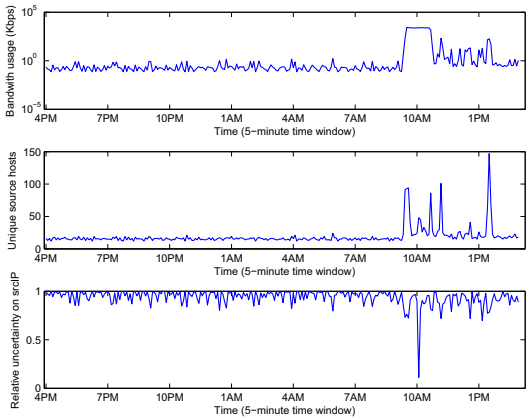

Fig. 3. An example of discovering anomalous traffic patterns through traffic summaries and behavior patterns provided by the HomeTPS system.

Figure 3 illustrates an example of applying HomeTPS system to detect interesting network events through a combination of traffic summaries and behavior patterns. The top figure shows the bandwidth usage of incoming traffic over a 24-hour time period for one Windows desktop in the home network, while the middle figure illustrates the unique source hosts that sent data packets to this desktop over time. Finally the bottom figure shows the distribution of network traffic among all unique source hosts over time using entropy measures from information theory [6]. The significant increase of bandwidth usage (shown in the top figure) starting from 9:20AM is caused by a mixture of a 90-minute Youtube video and Web surfing activities. At 10:05AM, we use the Nmap (Network Mapper) tool to simulate port scanning towards this desktop. The parallel increase of the unique source hosts are mostly the IP addresses of web servers that were visited during the time window. However, the significant drop of the relative uncertainty distribution on source hosts in the bottom figure indicates there exist one or a few source IP addresses, which have interacted with the device through a large number of network flows. The observation on the bottom figure successfully discovers the scanning traffic even though the traffic volumes measured in bytes and packets of the attack only account less than 1% and 5% of the overall traffic, respectively.

III. Demonstrations

Summarizing network traffic and dynamics: We will show real-time traffic summary reports for a simulated home network that includes a programmable home router, a traffic profiling server, and a home device. The report illustrates the top applications and end hosts based on network flows, packets and bytes, and also highlights the unusual ports or end hosts that exhibit significant increase or decrease in traffic volumes.

Monitoring traffic behavior: We will also demonstrate the discovery of traffic behaviors for end hosts and network applications via HomeTPS. The traffic behaviors leverage a variety of behavioral aspects from social, functional, application, volume, temporal dimensions.

Detecting anomalous traffic: To illustrate the capability of HomeTPS in detecting anomalous traffic patterns, we will use emulated attacks towards home network devices and show how HomeTPS discovers these anomalous behaviors.

References

[1] W. Edwards, R. Grinter, R. Mahajan, and D. Wetherall, "Advancing the State of Home Networking," *Communications of the ACM*, June 2011.
[2] N. Feamster, "Outsourcing Home Network Security," in *Proceedings of ACM SIGCOMM Workshop on Home Networks*, September 2010.
[3] P. De Lutiis, "Managing home networks security challenges: security issues and countermeasures," in *Proceedings of International Conference on Intelligence in Next Generation Networks*, October 2010.
[4] OpenWrt, "Linux distribution for embedded devices," openwrt.org/.
[5] K. Xu, F. Wang, and B. Wang, "Behavior Profiling and Analysis in Wireless Home Networks," in *Proceedings of IEEE Consumer Communications and Networking Conference*, January 2010.
[6] K. Xu, Z.-L. Zhang, and S. Bhattacharyya, "Internet traffic behavior profiling for network security monitoring," *IEEE/ACM Transactions on Networking*, vol. 16, pp. 1241–1252, December 2008.