Brave New World: Pervasive Insecurity of Embedded Network Devices

Ang Cui, Yingbo Song, Pratap V. Prabhu and Salvatore J. Stolfo

Intrusion Detection Systems Lab,
Columbia University, NY, USA
{ang,yingbo,pvp2105,sal}@cs.columbia.edu

Abstract. Embedded network devices have become an ubiquitous fixture in the modern home, office as well as in the global communication infrastructure. Devices like routers, NAS appliances, home entertainment appliances, wifi access points, web cams, VoIP appliances, print servers and video conferencing units reside on the same networks as our personal computers and enterprise servers and together form our world-wide communication infrastructure. Widely deployed and often misconfigured, they constitute highly attractive targets for exploitation. In this study we present the results of a vulnerability assessment of embedded network devices within the world's largest ISPs and civilian networks, spanning North America, Europe and Asia. The observed data confirms the intuition that these devices are indeed vulnerable to trivial attacks and that such devices can be found throughout the world in large numbers.

Key words: Router insecurity, network webcams, print servers, embedded device management interface exploitation, default password

1 Introduction

Embedded network devices perform specific functions like routing, file storage etc. Competition among manufacturers demand that these products be produced with minimal time to market at the lowest cost possible. These common commodity products are often implemented without security in mind and reside on the same networks as general purpose computers, making them attractive targets for exploitation. Once compromised, communication devices like routers, voip appliances, and video conferencing units can be used to quietly intercept and alter the traffic they carry. Nearly all embedded network devices contain a network interface which can be used to perform layer-2 and layer-3 attacks on the rest of the network. Since host based protection schemes for embedded devices generally do not exist today and network based protection schemes (802.1X etc) often intentionally exclude such devices administratively, exploitation and root-kitting[1] of these devices proves to be very advantageous to the attacker.

[1] The companion paper to this field survey will detail Doppelgänger; a semi-virtualized exploitation method for root-kitting heterogeneous embedded devices in a device and operating system agnostic manner.

2 Methodology

This paper presents preliminary results from our larger communications insecurity study by scanning, on a global scale, for perhaps the simplest attack possible; publicly accessible administrative interface with default password. We targeted the largest ISP networks in North America, Europe, and Asia, scanning and cataloging popular network appliances accessible over the internet. Out of all discovered devices, we then tabulated the number of such devices which are configured with their factory default administrative passwords. This data is then broken down by device types (Linksys, Polycom, Cisco etc), device class (Consumer, Enterprise, VOIP etc) and by geographical region (Zipcodes within the US and by Country world-wide).

Total IPs Scanned	Webservers	Telnet Servers	Devices Targeted	Vul. Devices Found
85.7 Million	1.1 Million	800 Thousand	105,357	3,847

Table 1. Key scan statistics thus far.

Enterprise Devices	VOIP Devices	Consumer Devices
2.46%	19.21%	41.62%

Table 2. Vulnerability rate by device class.

3 Findings

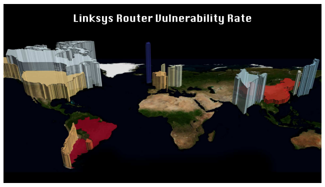

Fig. 1. Linksys vul. distribution.

JPN	CAN	IND	KOR
75.0%	60.0%	57.1%	57.1%
HUN	AUT	NLD	USA
54.5%	50.0%	48.6%	38.5%
CZE	FRA	URY	CHN
38.5%	34.2%	18.9%	10.0%

Fig. 2. Linksys vul. by country.

It is possible to draw several high level conclusions from the observed data. **Insecurity is pervasive world-wide**: Vulnerable devices can be found in significant numbers in all parts of the world covered by our scan. The double digit vulnerability rates suggest that a large botnet can be created by constituting only embedded network devices. [1]. **Geographical variations exist**: We found significant geographical concentrations of vulnerable devices of several types. This is undoubtedly related to the targeted markets of these devices. **Consumer devices are most vulnerable**: Looking at the vulnerability rates between consumer and enterprise devices world-wide, we see a significant difference between 45.62% versus 2.46%.

Detailed findings of our vulnerability assessment will be published in it's entirety upon the completion of the global scan.

References

1. DroneBL: Dd-wrt botnet http://dronebl.org/blog/8.