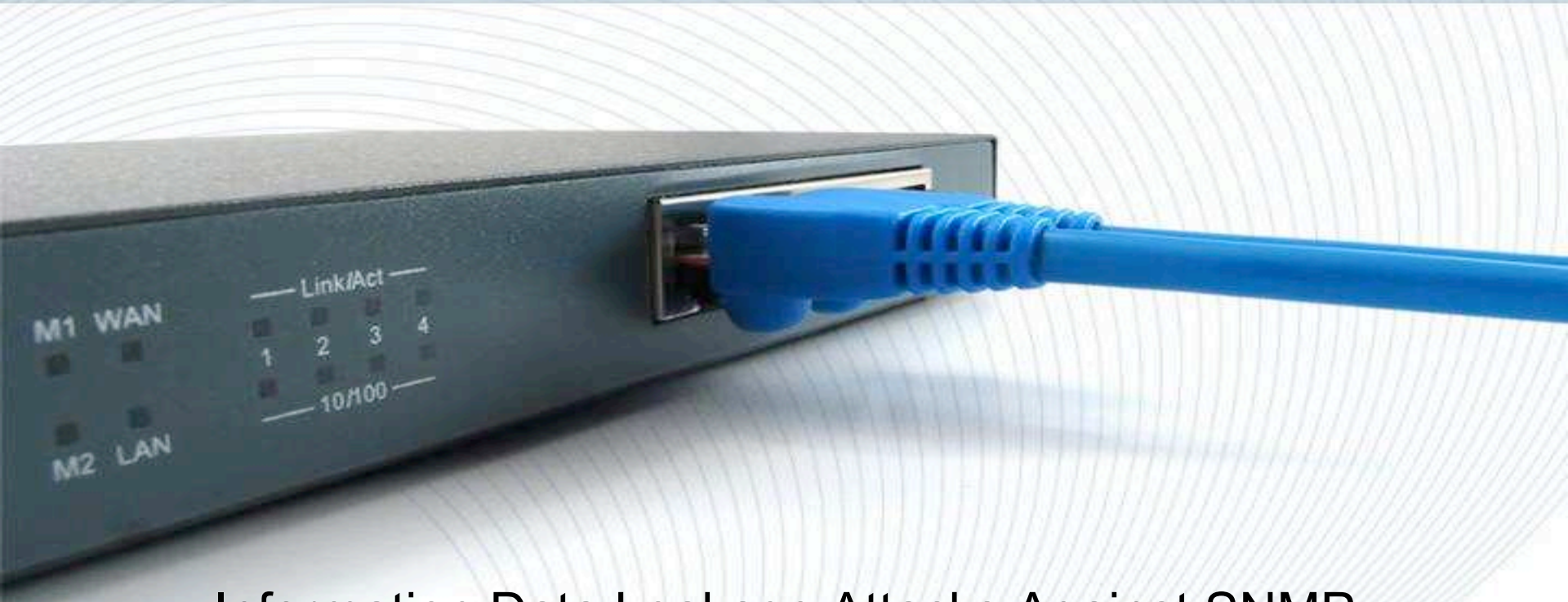
Simple Network Management Pwnd



Information Data Leakage Attacks Against SNMP

Introduction

Deral Heiland
deral_heiland@rapid7.com
dh@layereddefense.com
@Percent_X

Matthew Kienow
mkienow@inokii.com
@HacksForProfit

RAPID7

Why

- Add value
- Discover
- Exploit
- Curiosity

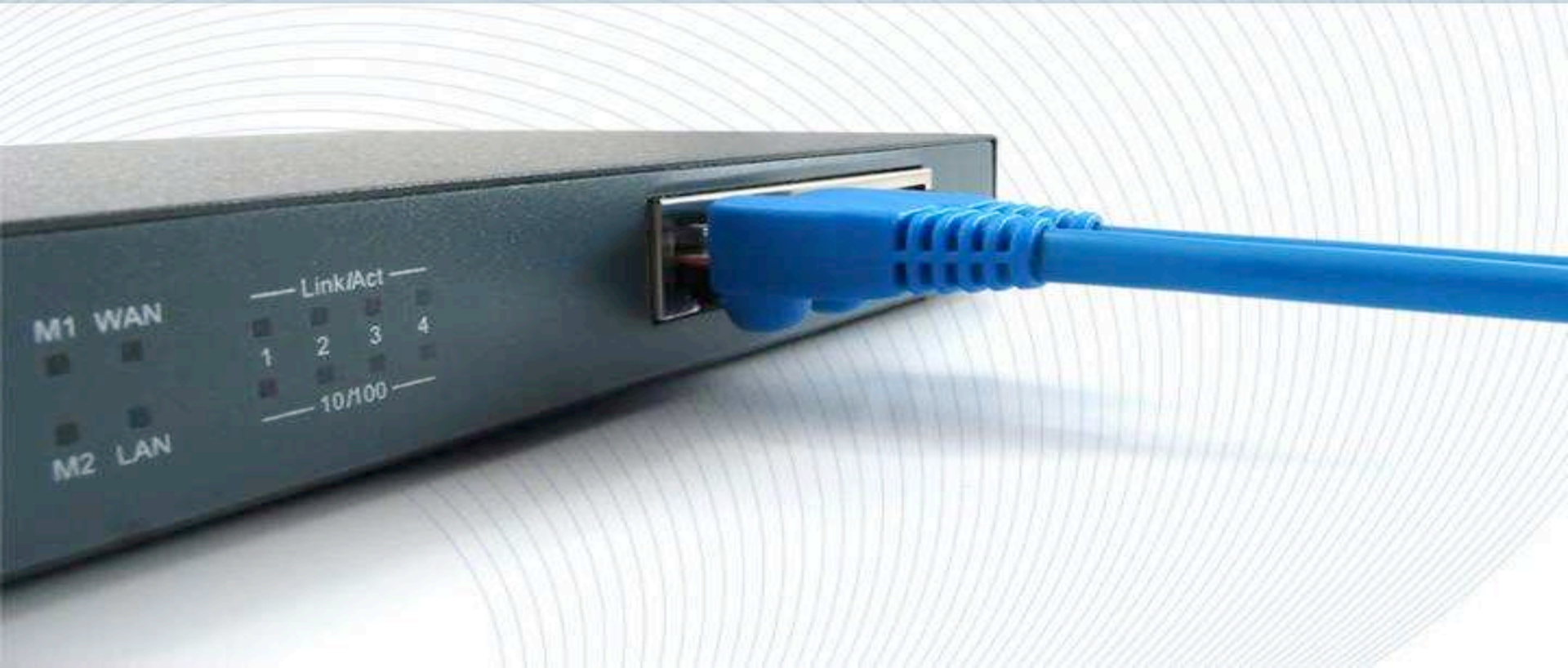
Why

SHODAN STATISTICS SNMP

7,205,555

- Brazil 2,423,559
- India 638,228
- United States 577,780
- Turkey 263,700
- France 45,039

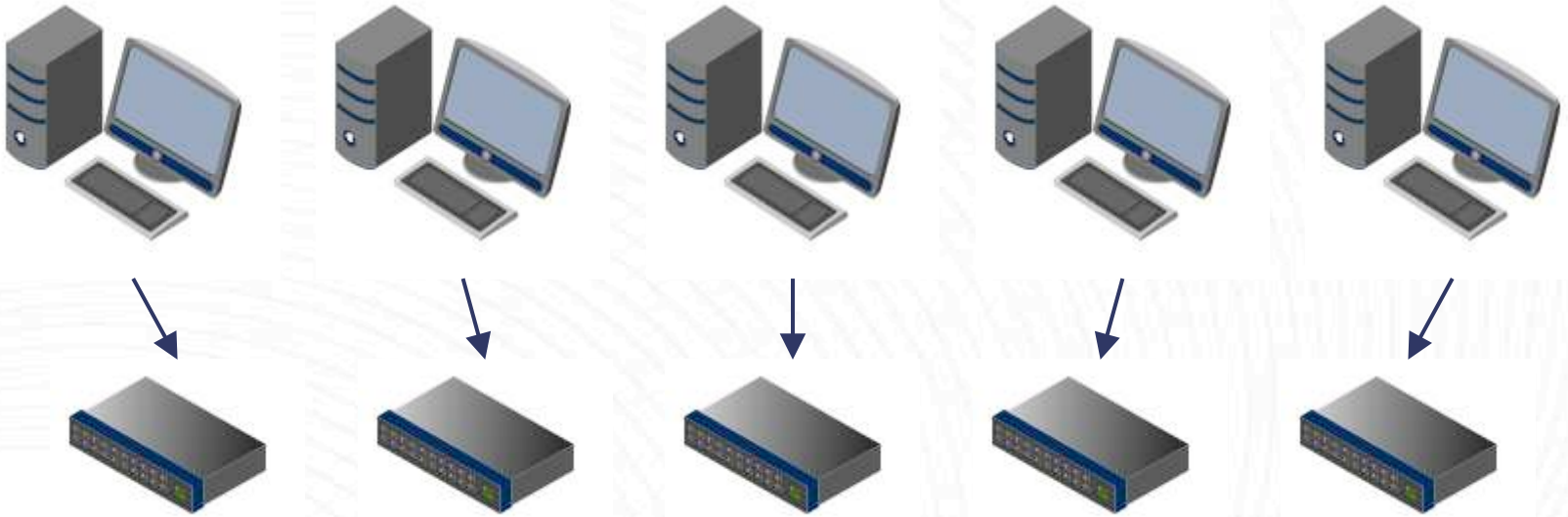
Introduction to SNMP



Simple

Why do we need SNMP?

Simple



Network Management

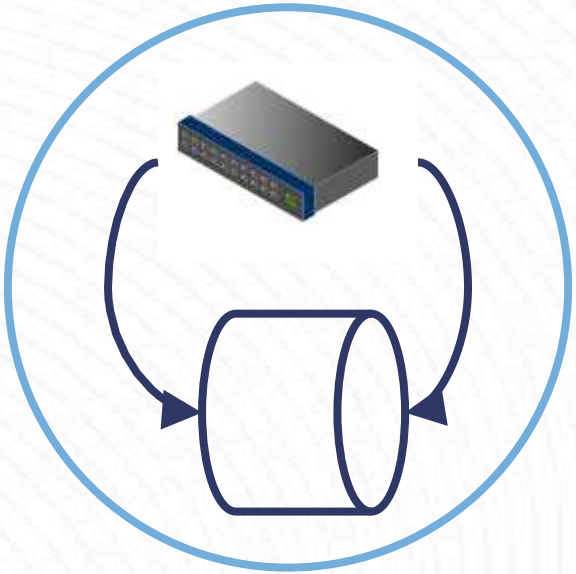
Monitoring

Managing

Manager

Network Management

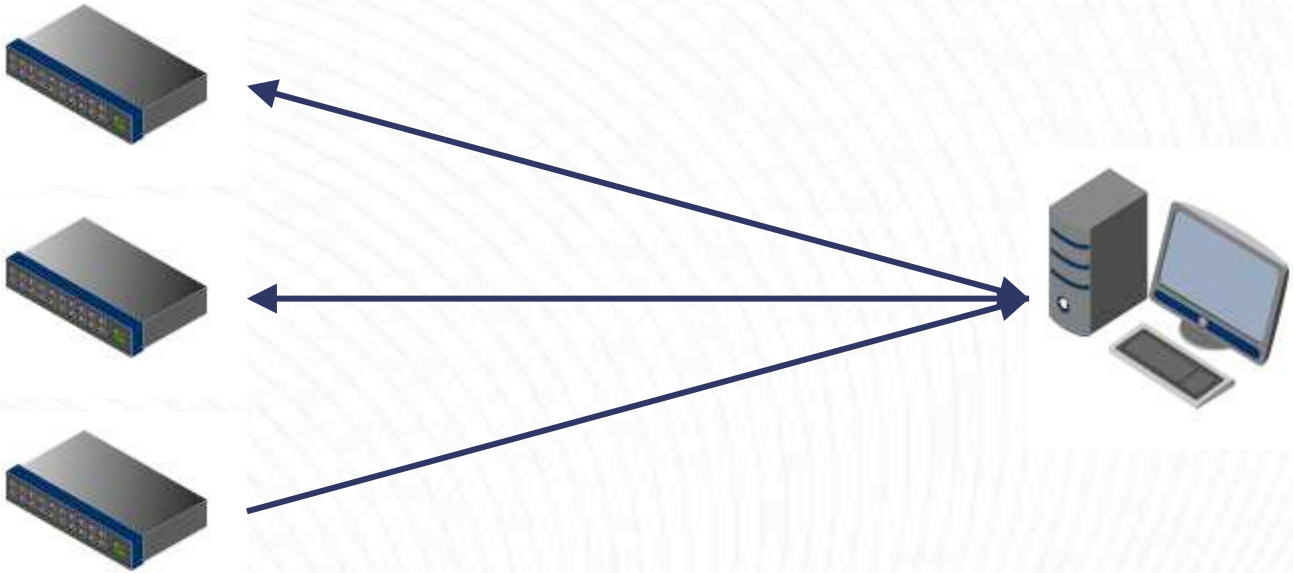
Tracking



Updating

Agent

Network Management



Communication

Protocol

- Provides management standards
- Transport protocol normally UDP
- Agent listens on port 161
- Manager listens on port 162

SNMP Version 1

Messages / Protocol Data Units (PDUs)

- Manager to Agent
  1. GetRequest
  2. GetNextRequest
  3. SetRequest
- Agent to Manager
  4. GetResponse
  5. Trap

GetRequest Message

1. Manager wants to get the value of the sysDescr and sysUpTime objects
2. Manager creates a GetRequest message

SNMPv1 Common PDU Format

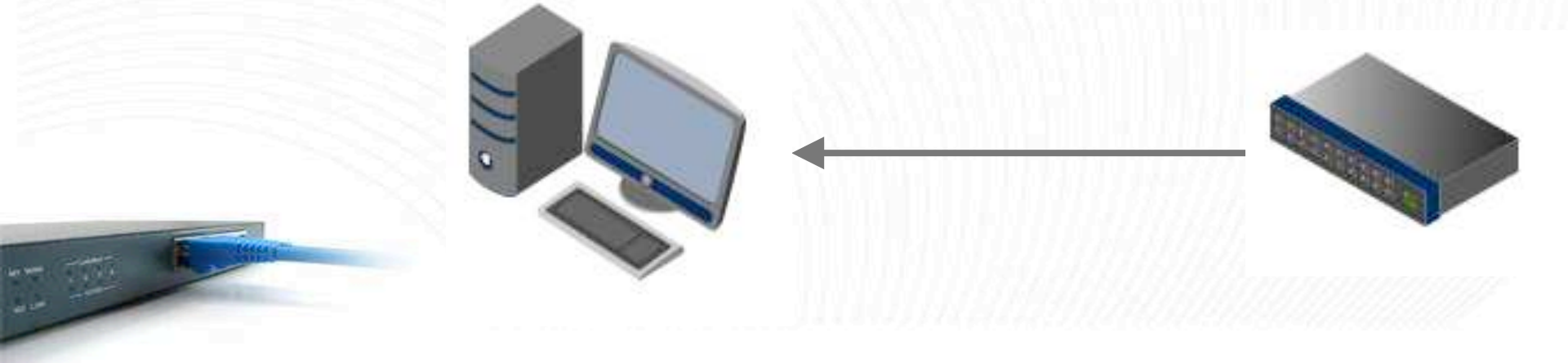
Version
Community
PDU Type (0-3)
Request Identifier
Error Status
Error Index
Variable Bindings Object 1: Value 1, …, Object X: Value X

GetRequest Message

3. Manager sends GetRequest message to router

GetRequest Message

4. Agent on router creates a GetResponse message with the values of the requested variables
5. Agent sends the message to the manager



SNMP Version 1

Messages / Protocol Data Units (PDUs)

- Manager to Agent
  1. GetRequest
  2. GetNextRequest
  3. SetRequest
- Agent to Manager
  4. GetResponse
  5. Trap

SNMP Version 2

Major Enhancements

- Addition of Messages / Protocol Data Units (PDUs)
  - GetBulkRequest - efficient retrieval of many variables in single request
  - InformRequest - acknowledged event notification

SNMP Version 2

Major Enhancements

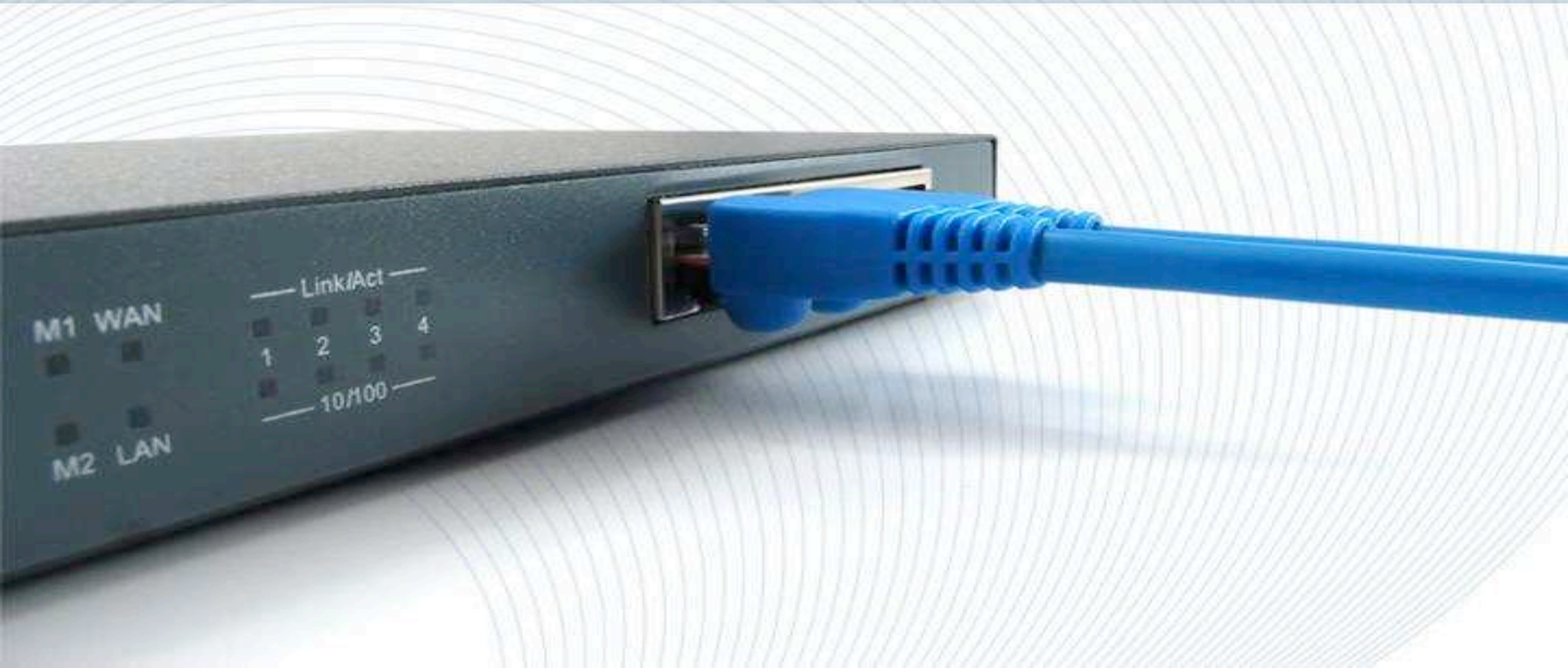
- Security enhancements
  - Party-Based SNMP Version 2
  - Community-Based SNMP Version 2 (SNMPv2c)
  - User-Based SNMP Version 2 (SNMPv2u)

SNMP Version 3

Major Enhancements

- Security Model
  - Authentication
  - Encryption
  - Integrity
- Access Control Model

Introduction OIDs and MIBs



Introduction OIDs and MIBs

How do we enumerate specific data using SNMP?

Introduction OIDs and MIBs

“**Management Information Base (**MIB) is a file that contains definitions of management information so that networked systems can be remotely monitored, configured, and controlled.”

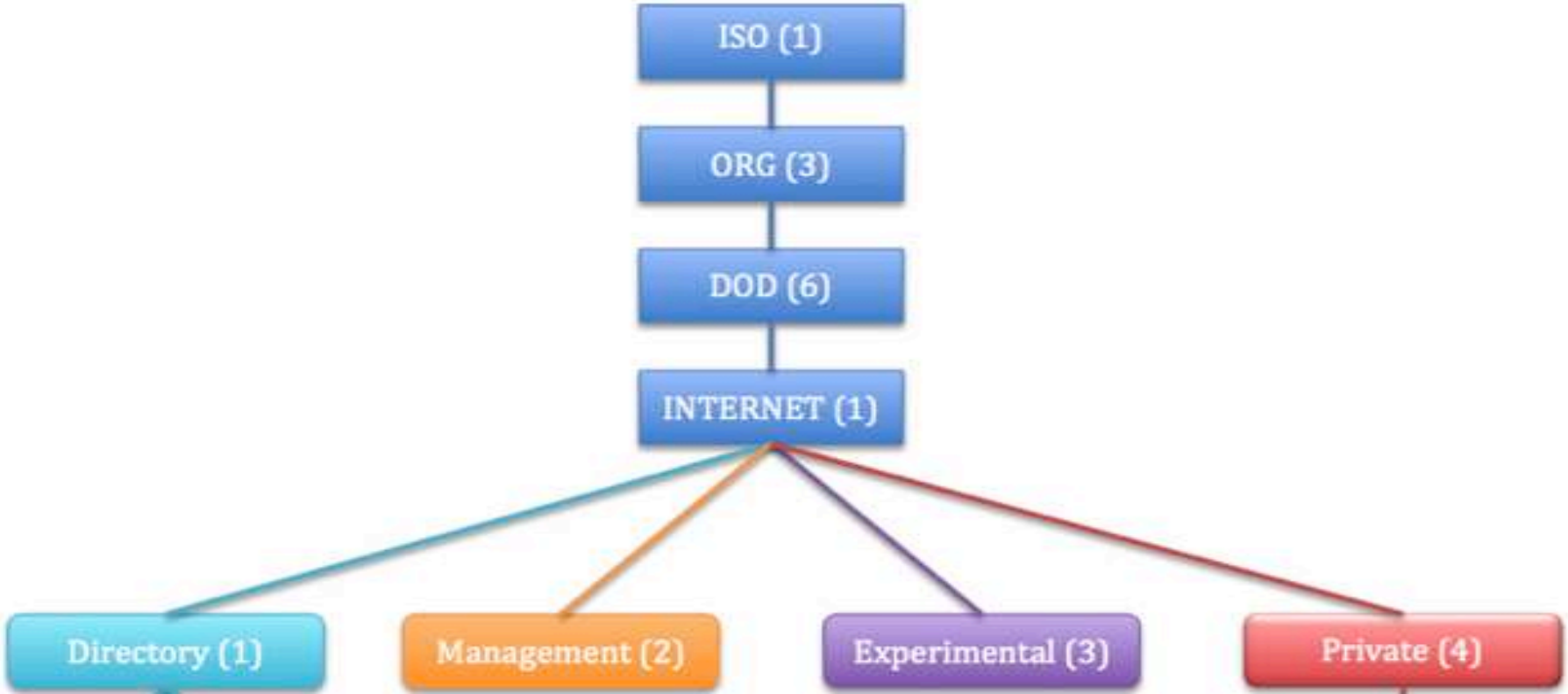
Introduction OIDs and MIBs

“**Object Identifier (OIDs)** point to individual network objects that are maintained in a database called a Management Information Base“

Introduction OIDs and MIBs

- OIDs utilize a dotted list notation
  - 1.3.6.1 = iso.org.dod.internet
  - Universally unique

Introduction OIDs and MIBs



Introduction OIDs and MIBs

Number of Network Interfaces on a Device

1.3.6.1.2.1.2.1

ifNumber (1)

Introduction OIDs and MIBs

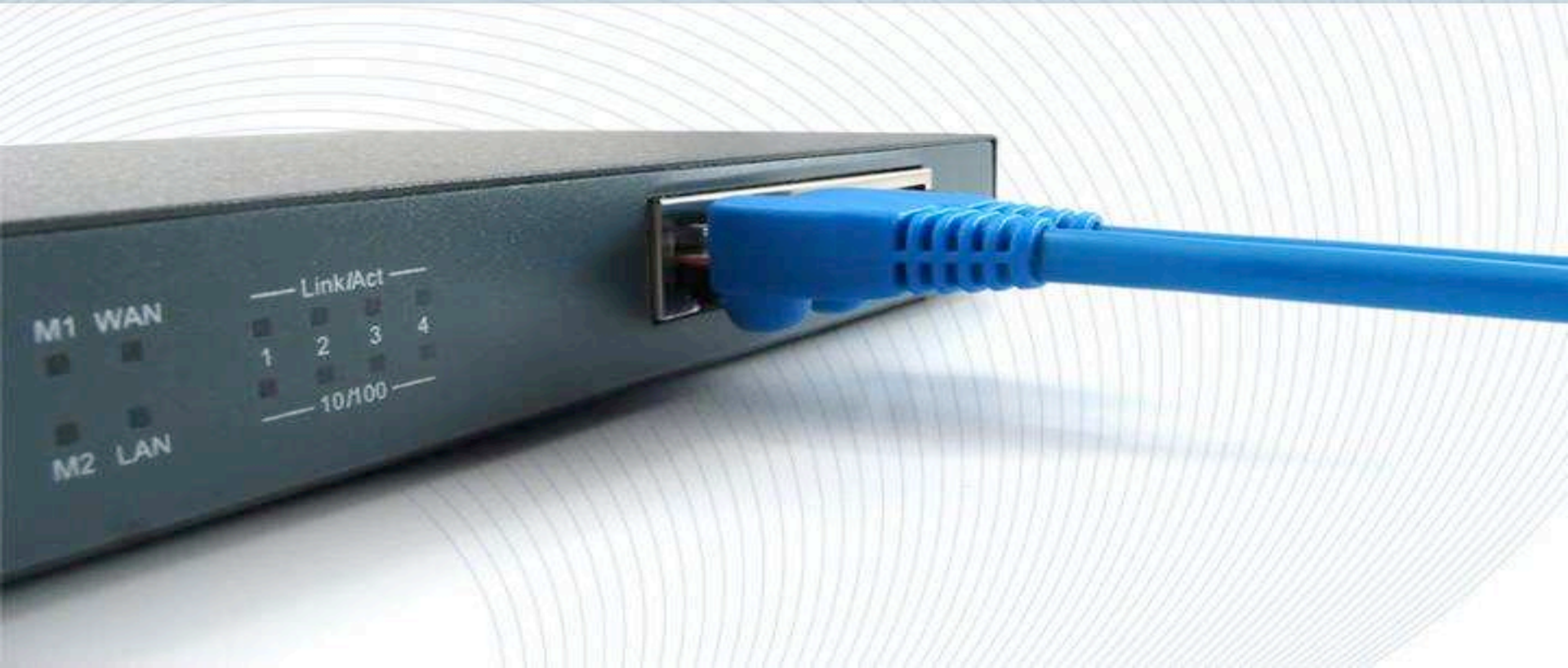
- Enterprise MIBs
  - 1.3.6.1.4.1
  - iso.org.dod.internet.private.enterprise
- Individual enterprises are assigned a number by Internet Assigned Numbers Authority (IANA)

http://www.iana.org/assignments/enterprise-numbers/enterprise-numbers

Introduction OIDs and MIBs

1.3.6.1.4.1.2	IBM
1.3.6.1.4.1.9	ciscoSystems
1.3.6.1.4.1.11	Hewlett-Packard
1.3.6.1.4.1.304	Farallon Computing, Inc.
1.3.6.1.4.1.1991	Brocade Communication Systems, Inc.
1.3.6.1.4.1.4491	Cable Television Laboratories, Inc.
1.3.6.1.4.1.4684	Ambit Microsystems Corporation
1.3.6.1.4.1.43555	LayeredDefense Deral Heiland

SOHO Device Attacks



Exploits & Related Attack Vectors

- Initial research focused on cable / DSL modems
  - Easily obtainable devices
  - Low cost
- Devices examined
  - Netopia/Motorola/Arris
  - Ambit/Ubee
  - Netmaster

Exploits & Related Attack Vectors

- Modems with WiFi builtin frequently expose
  - Wireless keys
  - SSIDs
  - Interface credentials

Manual Information Extraction Demo

Exploits & Related Attack Vectors

Username:	1.3.6.1.4.1.4491.2.4.1.1.6.1.1.0
Password:	1.3.6.1.4.1.4491.2.4.1.1.6.1.2.0
WEP Key Index:	1.3.6.1.4.1.4684.38.2.2.2.1.5.4.2.3.1.2.12
WPA PSK:	1.3.6.1.4.1.4491.2.4.1.1.6.2.2.1.5.12
SSID:	1.3.6.1.4.1.4684.38.2.2.2.1.5.4.1.14.1.3.12

Ubee DDW3611

Automated Information Extraction Demo

Exploits & Related Attack Vectors

Password:	1.3.6.1.4.1.4491.2.4.1.1.6.1.2.0
SSID:	1.3.6.1.4.1.4115.1.20.1.1.3.22.1.2.12
WPA PSK:	1.3.6.1.4.1.4115.1.20.1.1.3.26.1.2.12
WEP Key 64-bit Index:	1.3.6.1.4.1.4115.1.20.1.1.3.24.1.2.1
WEP Key 128-bit Index:	1.3.6.1.4.1.4115.1.20.1.1.3.24.1.2.1

ARRIS DG950A

Exploits & Related Attack Vectors

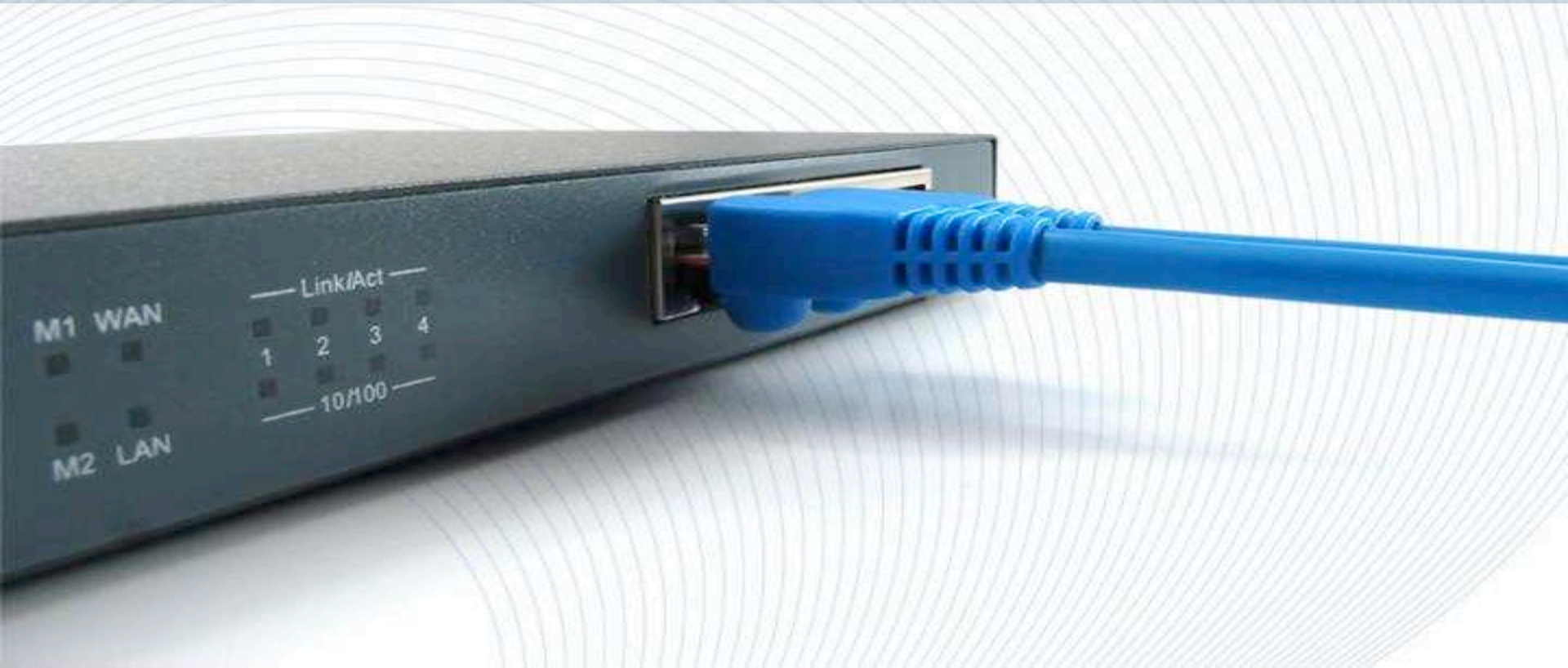
- Modems Identified leaking data
  - Ambit U10C019 (2,285)
  - Ubee DDW3611
  - Netopia 3347 series (40,444)
  - Arris DG950A (19,776)
  - Motorola/Arris SBG-6580 (97)
  - Netmaster CBW700N (114,265)

176,867

Observations and Trends

- Internet Service Providers (ISP) have poorly configured SNMP to manage cable/dsl modems
- A decrease in exploitable devices
  - Older devices are replaced
  - Newer deployments better secured

Enterprise Device Attacks



Enterprise Device Attacks

- SNMP is available on all enterprise devices
- Often found enabled by default
- Almost as often configured with community strings of public and private

Enterprise Device Attacks

Brocade ServerIron ADX 1016-2-PREM

Demo

Brocade Load Balancer

Brocade ServerIron ADX 1016-2-PREM

Shodan results for ServerIron (826)

USERNAME	1.3.6.1.4.1.1991.1.1.2.9.2.1.1
PWD HASHES	1.3.6.1.4.1.1991.1.1.2.9.2.1.2

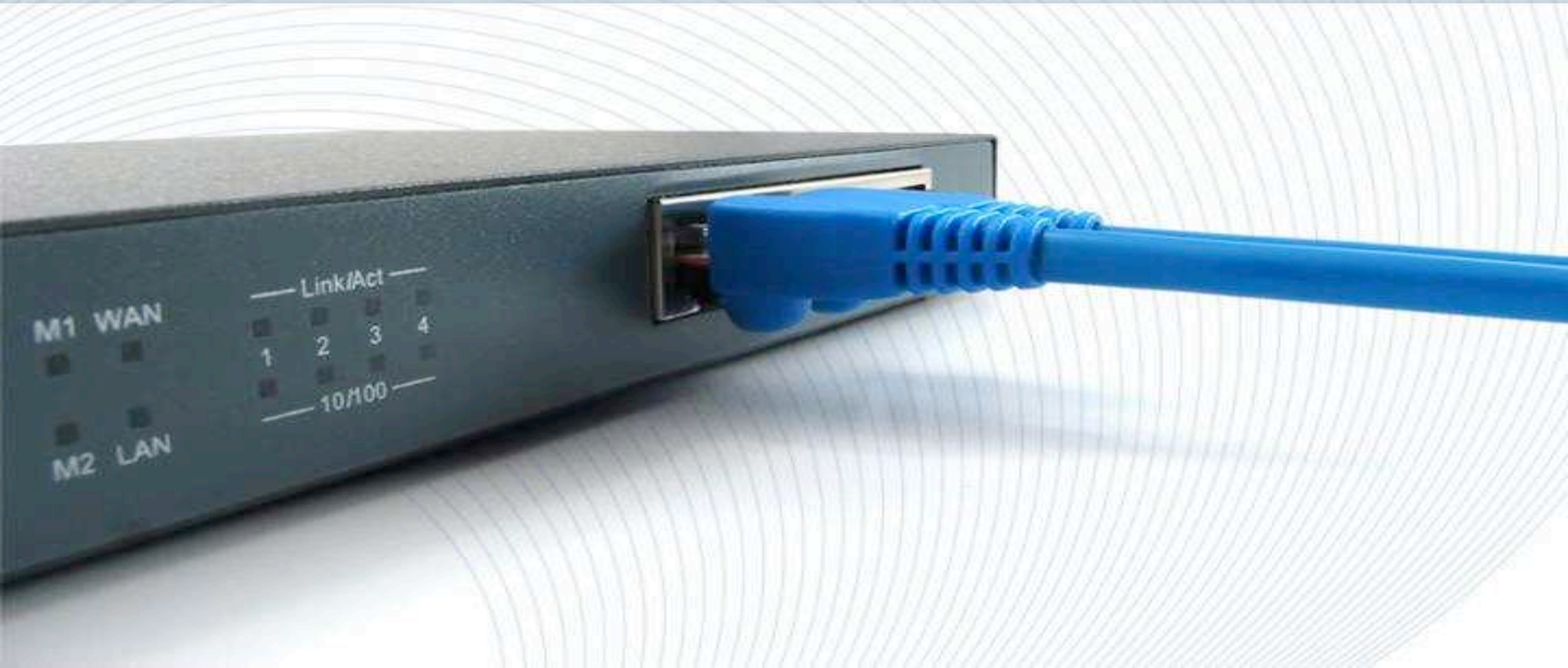
Enterprise Device Attacks

- Kyocera printers (Various models)
  - Independently discovered by both Artyon Breus and Chris Schatz

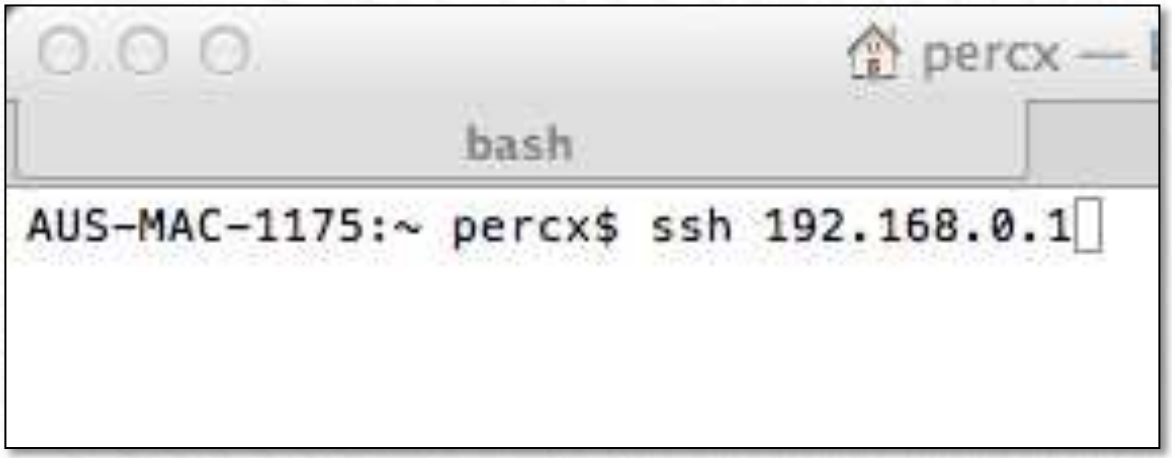
- SMB Path: 1.3.6.1.4.1.1347.42.23.2.4.1.1.2.x.1
- SMB Host: 1.3.6.1.4.1.1347.42.23.2.4.1.1.3.x.1
- SMB Port: 1.3.6.1.4.1.1347.42.23.2.4.1.1.4.x.1
- SMB Login: 1.3.6.1.4.1.1347.42.23.2.4.1.1.5.x.1
- SMB Password: 1.3.6.1.4.1.1347.42.23.2.4.1.1.6.x.1

X= user number

Information Harvesting



Log Data Extraction Attacks



Demo

Log Data Extraction Attacks

- Logs viewable via SNMP
- Successful logins
  - Identify valid accounts
  - Identify host they authenticated from
- Failed logins
  - Oops... I just entered my password in the user field
  - Maybe an injection point for XSS in the web viewed logs

Log Data Extraction Attacks

DEMO

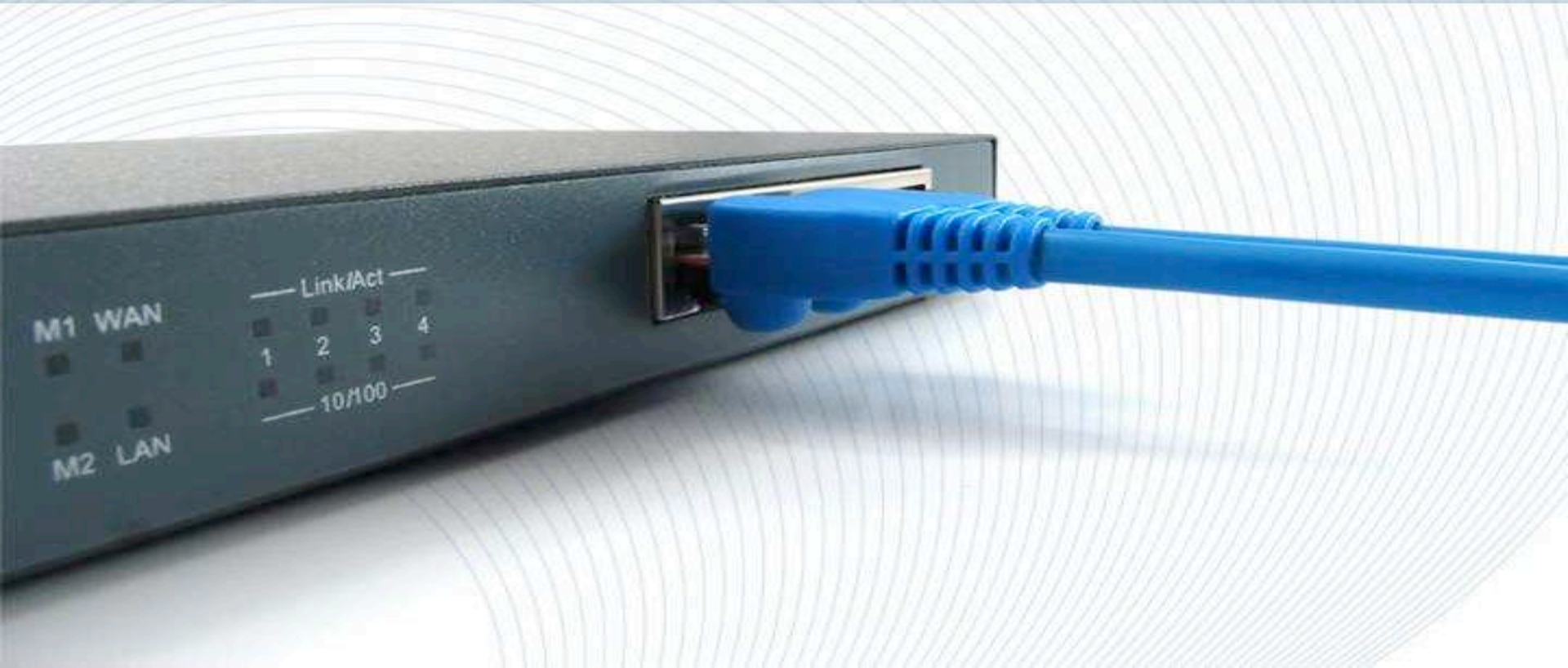
Log Data Extraction Attacks

- When encountering devices on a pen-test
  - Alway check to see whether SNMP is enabled and accessible
  - Snmp(bulk)walk device and analyze prior to engaging the device with brute force attacks (telnet, ssh, web, etc.)
  - Avoid overwriting usable data

Log Data Extraction Attacks

- Sample list of device with SNMP stored logs
  - Netgear ProSafe GSM7328Sv2 Managed Switch
  - Smart IP Microwave Radio
  - Netopia 33xx

Automated Information Harvesting



Automated Information Harvesting

- Large amounts of data
- Unknown meaning of data
- Limited time to analyse

Automated Information Harvesting

- How do we gather useful information?
  - Snmp(bulk)walk all devices
  - Parse for keyword and patterns

Automated Information Harvesting

- snmpbw.pl (Still work in progress)
  - Perl script
  - Multithreaded
  - Runs snmpbulkwalk against target list
  - https://github.com/dheiland-r7/snmp

Automated Information Harvesting

- snmpprs.pl (Still work in progress)
  - Perl script
  - Parses snmpwalk data for information
  - https://github.com/dheiland-r7/snmp

Automated Information Harvesting

- Data harvest
  - usernames
  - password or hashes
  - SNMP community strings
  - network infrastructure and VLANs information

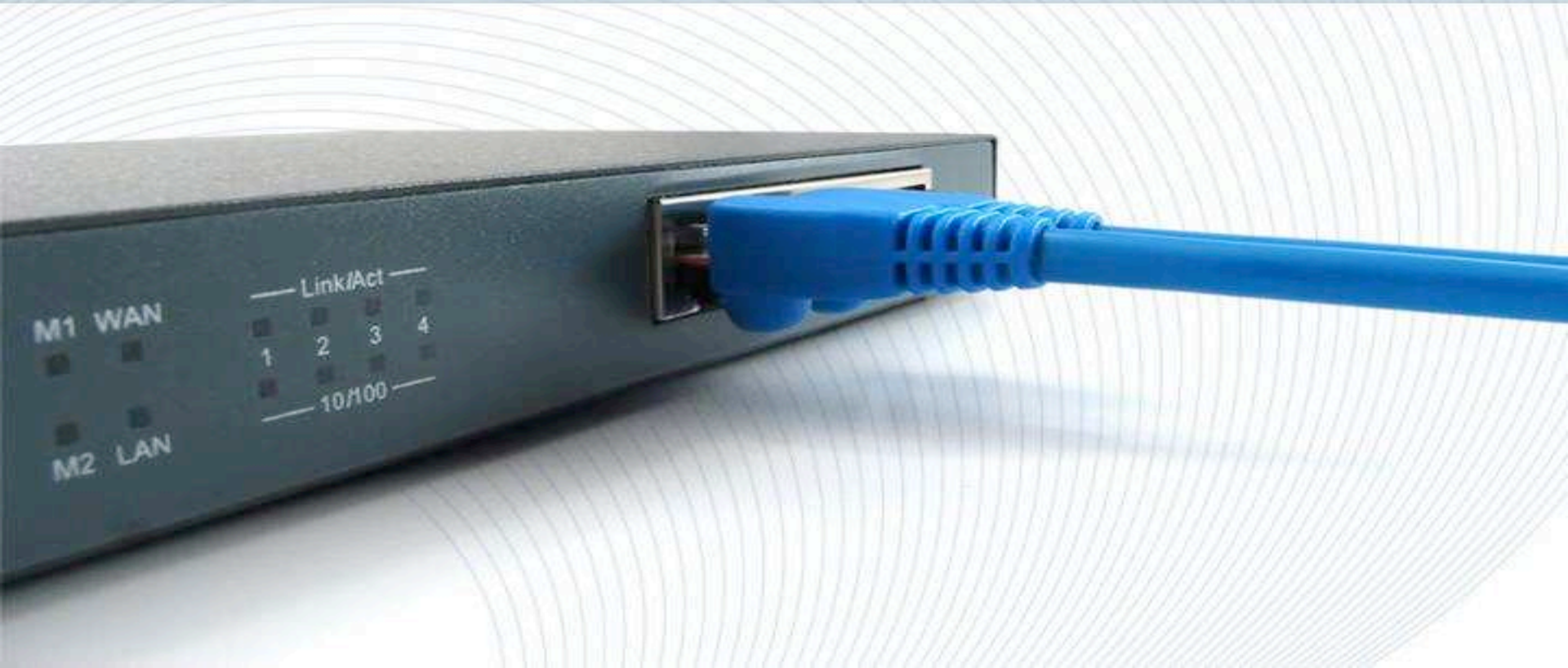
Automated Information Harvesting

- Samples
  - \$[1-6]\$[0-9a-zA-Z.$/]\{31\}
  - \"[0-9A-Fa-f]\{32\}\”
  - [a-zA-Z.]@[a-zA-Z].[cegmnort]
  - traphost
  - admin, Admin, root
  - fail, success, logging

Automated Information Harvesting

DEMO

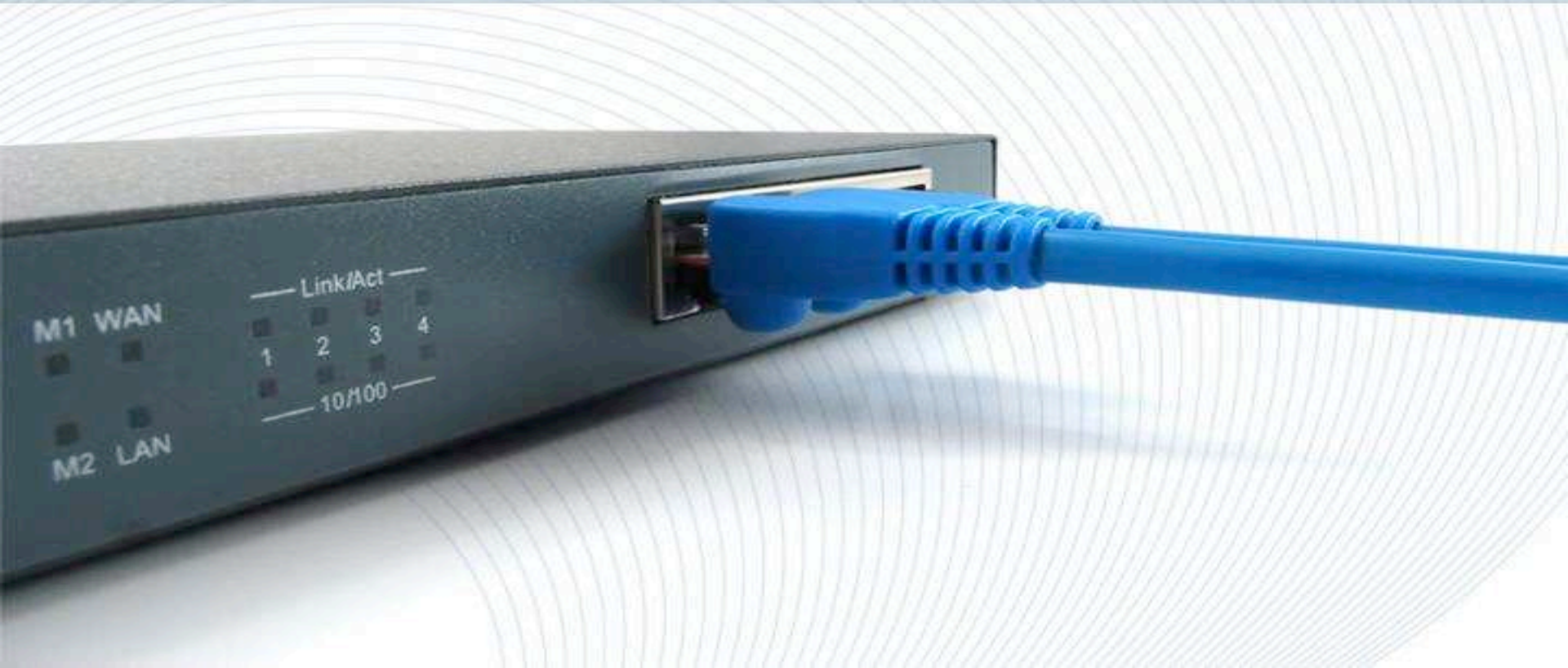
Other Data Points of Interest



Other Data Points of Interest

- SNMP DoS
  - Earliest identified DoS POC dated 2005
    - http://packetstormsecurity.com/files/36070/snmpdos.c.html
  - Attacker can direct responses to a target since UDP is connectionless, allowing spoofed IP address
  - GetBulkRequest message is used for reflected amplification attacks

SNMP Security Best Practices



SNMP Security Best Practices

- Manufacture:
  1. SNMP disabled by default
  2. Move away from SNMPv1 and SNMPv2c
  3. MIB objects should not contain any authentication data
     - Passwords, password hashes, security keys, usernames or community strings
     - Should only contain data related to the operational parameters of the device

SNMP Security Best Practices

- End User:
  1. SNMP if not in use should be disabled on all devices prior to deployment.
  2. SNMP community strings should be a minimum of 20 characters, alphanumeric upper and lower case with special characters and contain no dictionary words.

SNMP Security Best Practices

- End User:
  3. SNMP community strings public and private should not be the same
  4. SNMP community strings should differ based on the different security levels of the devices. Example: SNMP community string on your IP camera should not be the same as your router/switches/firewalls.

Conclusion

Deral Heiland
deral_heiland@rapid7.com
dh@layereddefense.com
@Percent_X

Matthew Kienow
mkienow@inokii.com
@HacksForProfit

RAPID7

References

- http://www.bitag.org/documents/SNMP-Reflected-Amplification-DDoS-Attack-Mitigation.pdf
- http://www.prolexic.com/kcresources/white-paper/white-paper-snmp-ntp-chargen-reflection-attacks-drdos/An_Analysis_of_DrDoS_SNMP-NTP-CHARGEN_Reflection_Attacks_White_Paper_A4_042913.pdf

Exploit References

- https://community.rapid7.com/community/metasploit/blog/2014/05/15/r7-2014-01-r7-2014-02-r7-2 14-03-disclosures-exposure-of-critical-information-via-snmp-public-community-string
- https://community.rapid7.com/community/metasploit/blog/2014/08/21/more-snmp-information-leaks-cve-2014-4862-and-cve-2014-4863
- http://seclists.org/fulldisclosure/2014/May/79