SNMP Security for Campus Networks and Systems

Internet2 Technology Exchange
Indianapolis, IN, Wed Oct 29th, 2014

White River Ballroom D, 1:30-2:15 PM

Joe St Sauver, Ph.D. (joe@stsauver.com)

https://www.stsauver.com/joe/snmp-security/

Section 1. The Legacy of "Security As An Afterthought" For A Key/Ubiquitous Protocol

Organization for Standardization, International Standard 8825, December 1987.

[11] Postel, J., "User Datagram Protocol", RFC 768, USC/Information Sciences Institute, November 1980.

Security Considerations

Security issues are not discussed in this memo.

SNMP Security Has Always Been An Afterthought

- In a world where security really needs to be designed in from the beginning, SNMP has always been a protocol where security was largely overlooked or ignored.

- This can be clearly seen in the excerpt from RFC 1157 quoted on the intro to this section:

> "Security issues are not discussed in this memo."

Nonetheless, SNMP *Is* Ubiquitous

- Seemingly every device on the network supports SNMP.

- This is, in many ways, laudable: you can centrally manage "everything."

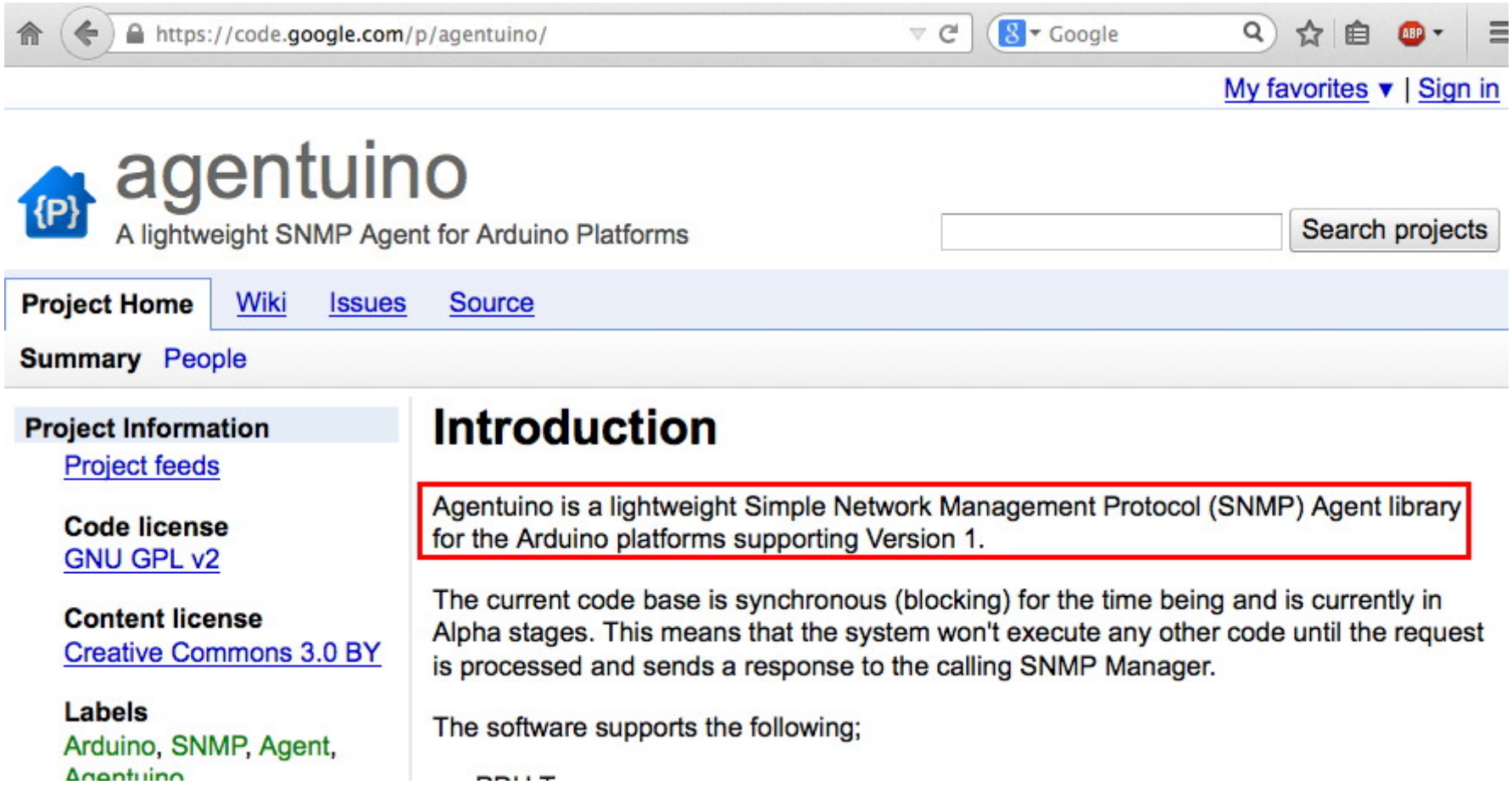
- This is, in many OTHER ways, horrific:

  -- least-common-denominator protocol implementations tend to lack critical features (like security and privacy)

  -- "on by default" rather than "on only where absolutely needed" increases your attack surface

  -- many unexpected side effects surface seemingly **everywhere.**

SNMP, Even on The Smallest/Simplest of Devices



If you're not familiar with the Arduino, see http://arduino.cc/

SNMP on Core Strategic Technologies (e.g., SDN)

https://wiki.opendaylight.org/view/SNMP4SDN:Architecture_and_Design

Overview

We propose a southbound plugin that can control the off-the-shelf commodity Ethernet switches for the purpose of building SDN using Ethernet switches. For Ethernet switches, forwarding table, ACL, and VLAN table are where one can install the flow configuration on, and this is done via SNMP and CLI in the proposed plugin. In addition, extensions to the SAL configuration APIs are needed to provide additional API to support some settings, e.g. disabling STP and flooding, etc, which are required for Ethernet switches in SDN.

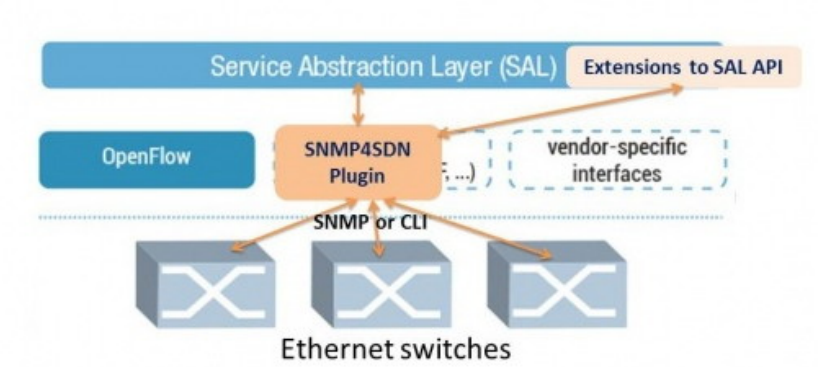


Figure. SNMP4SDN as a southbound plugin in OpenDaylight architecture

Functionality

For the SDN controller to support building an SDN using Ethernet switches, it needs to be able to configure flows on the Ethernet switches. In addition, in initial, it has to discover which switches are under its management and then can configure flows on them. Also, the connectivity topology among switches is necessary information for the controller and applications. In this plugin, flow configuration on Ethernet switch would be done via SNMP or CLI, switch discovery would be achieved via SNMP trap sent from the switch, and topology discovery would be resolved by reading LLDP data on the switches.

Flow configuration on Ethernet switch

A flow's configuration on an Ethernet switch could be implemented by configuring forwarding table, ACL, and VLAN, via SNMP or CLI.

SNMP on Non-Enterprise Devices, Too

http://krebsonsecurity.com/2014/06/they-hack-because-they-can/comment-page-1/

05 They Hack Because They Can

JUN 14

The Internet of Things is coming....to a highway sign near you? In the latest reminder that much of our nation's "critical infrastructure" is held together with the Internet equivalent of spit and glue, authorities in several U.S. states are reporting that a hacker has once again broken into and defaced electronic road signs over highways in several U.S. states.

Earlier this week, news media in North Carolina reported that at least three highway signs there had apparently been compromised and re-worded to read "Hack by Sun Hacker." Similar incidents were reported between May 27 and June 2, 2014 in two other states, which spotted variations on that message left by the perpetrator, (including an invitation to chat with him on Twitter).

Image: WNCN.

The attack was reminiscent of a series of incidents beginning two years ago in which various electronic message signs were changed to read "Warning, Zombies Ahead".

SNMP's Design Leverages UDP

- This means it's vulnerable to **spoofed traffic** if everyone doesn't do BCP38/BCP84 (and many still don't)

- This also means that it can act as a terrific **packet cannon**, potentially generating congestion-insensitive blasts of UDP packets at wire speed.

- But hey, what could go wrong? :-;

Why Pay Attention to SNMP Security Today?

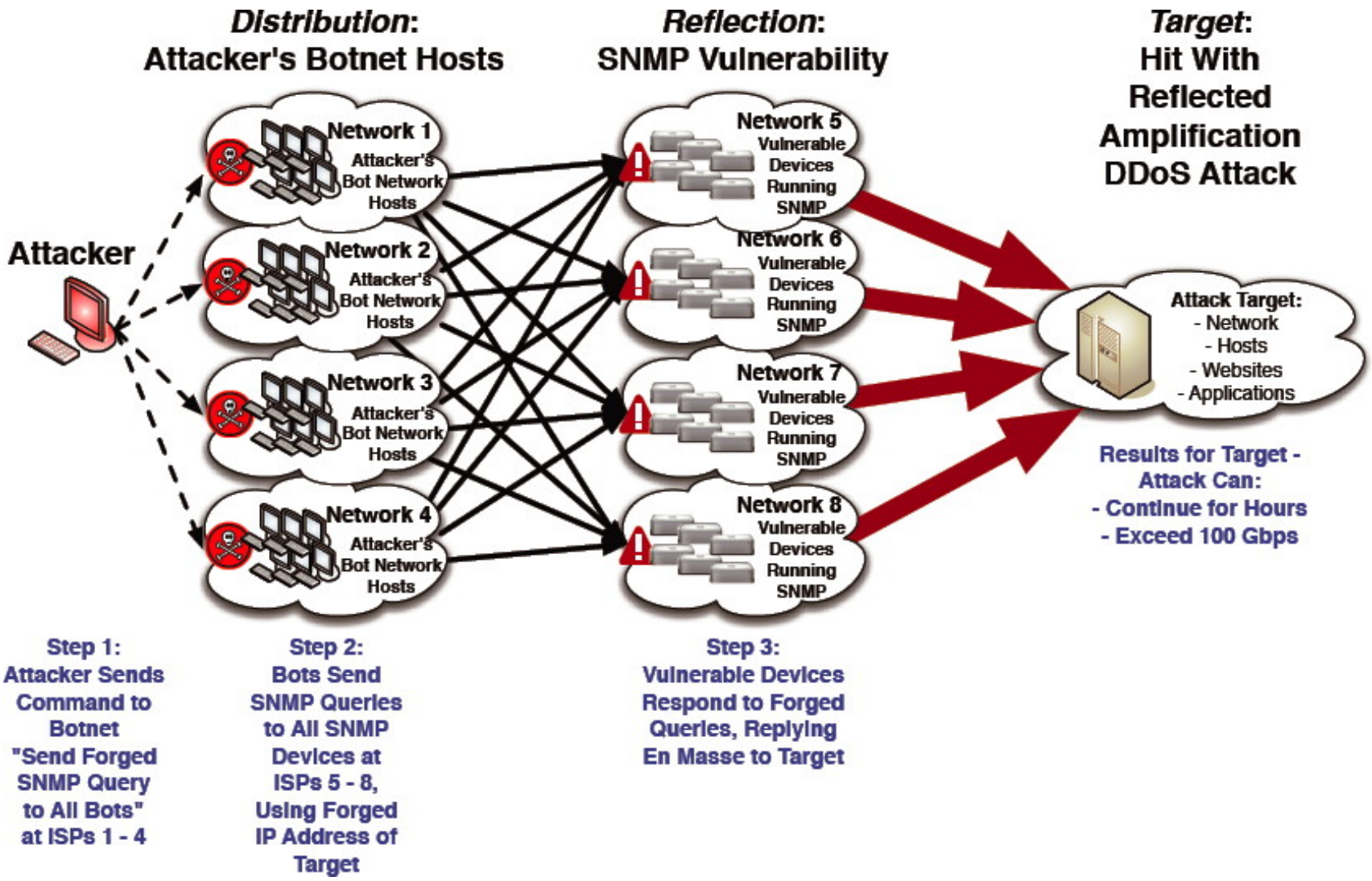
- SNMP is being attacked, **but it is also being used as a tool for attacking other sites (e.g., for conducting DDoS attacks).**

- If you run SNMP and end up hurting yourself, that's one thing. Your errors, your pain.

- If your SNMP problems affect others, that's something completely different and much more serious. Your mistake, community pain and suffering. That asymmetry is a big problem for me.

- **SNMP reflective amplification attacks** are quite similar to DNS, NTP and similar reflective amplification attacks, **but with far larger potential amplification factors**.

How An SNMP Reflection Attack Works



http://www.bitag.org/documents/SNMP-Reflected-Amplification-DDoS-Attack-Mitigation.pdf

SNMP Reflection Amplification Factor

- "... the laboratory setup was able to replicate requests and payloads. The tool produced a **request of 37 bytes** and an **amplified response of 51,722 bytes**, effectively replicating the SNMP reflection attack seen in the campaigns."

  "Threat Advisory: SNMP Reflection Attacks," http://www.prolexic.com/kcresources/prolexic-threat-advisories/prolexic-ddos-threat-advisory-snmp-reflector/TA-SNMP-Reflection-A4-052014.pdf

- Doing the math: 51,722/37=**1,397.9 amplification factor!**

- The attack tool in question is easily found on the Internet today.

SNMP Also Frequently Acts As A Routine "Built in Flaw/Point of Vulnerability"

- For example:

- **SNMP community strings brute forced** (presumably) as an entry point for further attacks against the SNMP-managed device
- In other cases, **SNMP can be just a little two willing to spill its guts about itself**
- SNMP as a **DoS vector against applications running on the managed device** (example: Squid)
- Attackers are even exploring attacks against basic device functions (such as packet forwarding) via **intentional device misconfiguration** via SNMP

- Some specific examples of these...

Spike In Brute Force Access Attacks

http://blogs.cisco.com/security/snmp-spike-in-brute-force-attempts-recently-observed/

SNMP: Spike in Brute-force Attempts Recently Observed

Scott Bradley | June 17, 2014 at 5:00 am PST

(2 Comments)

Simple Network Monitoring Protocol (SNMP) has been widely deployed as an important network management tool for decades, is a key component of scalable network device management, and is configurable in nearly all network infrastructure devices sold today. As with any management protocol, if not configured securely, it can be leveraged as an opening for attackers to gain access to the network and begin reconnaissance of network infrastructure. In the worst case, if read-write community strings are weak or not properly protected, attackers could directly manipulate device configurations.

Cisco has recently seen a spike in brute-force attempts to access networking devices configured for SNMP using the standard ports (UDP ports 161 and 162). Attacks we've observed have been going after well known SNMP community strings and are focused on network edge devices. We have been working with our Technical Assistance Center (TAC) to assist customers in mitigating any problems caused by the brute-force attempts.

http://www.securityweek.com/devices-leak-critical-information-snmp-public-community-string-researchers

According to Heiland, the Brocade device stores username and passwords hashes within the SNMP MIB [Management Information Base] tables at the following OID Indexes:

- Username: 1.3.6.1.4.1.1991.1.1.2.9.2.1.1
- Password hash: 1.3.6.1.4.1.1991.1.1.2.9.2.1.2

"The Brocade ServerIron load balancer has SNMP enabled by default," he explained. "The community string "public" is configured by default. Unless SNMP is disabled, or the public community string is changed, an attacker can easily extract the passwords hashes for an offline brute force attack."

The Ambit U10C019 and Ubee DDW3611 series of cable modems store the following information within the SNMP MIB tables at these OID [Object Identifier] Indexes:

U10c019

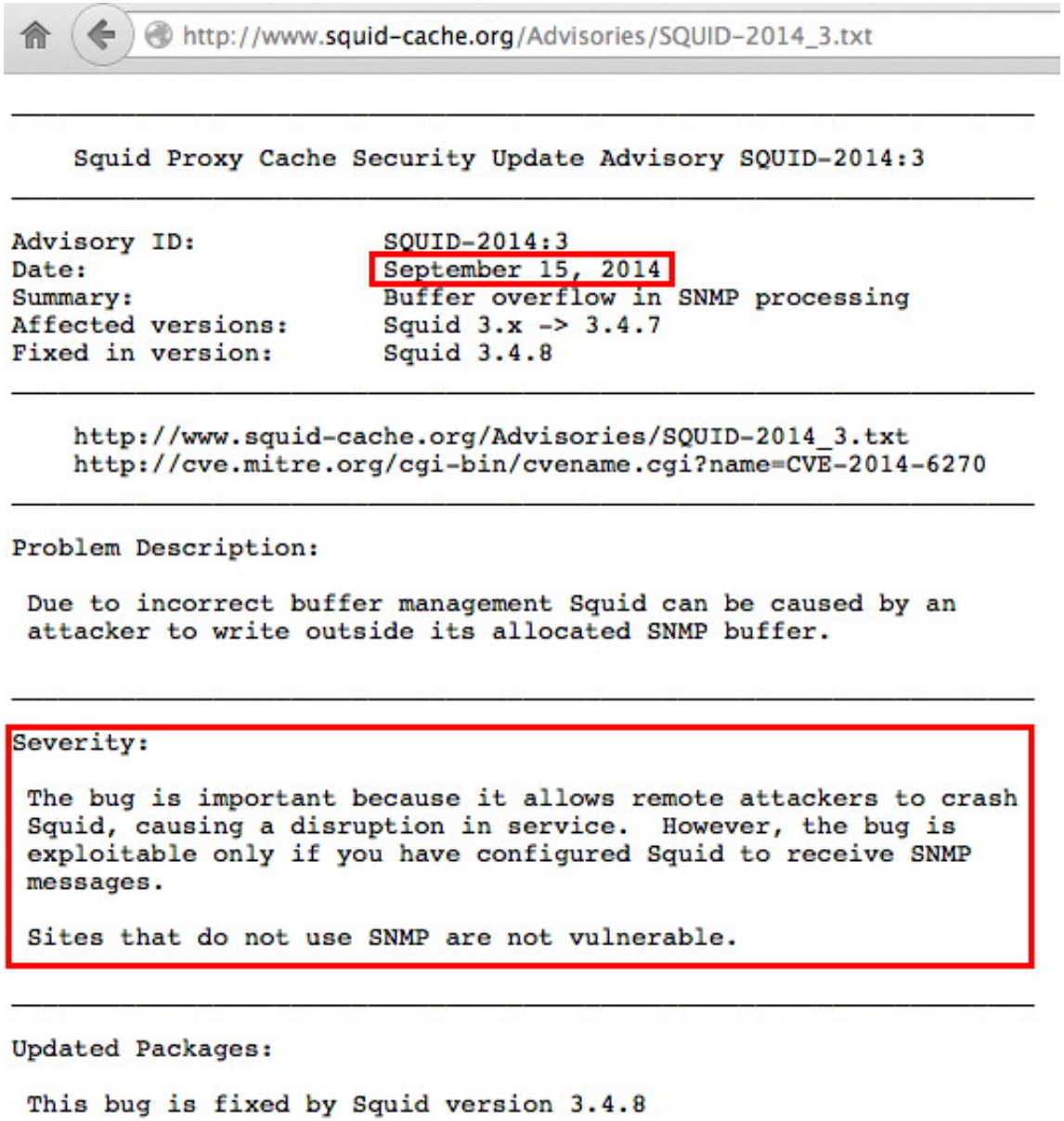
- Username: 1.3.6.1.4.1.4684.2.17.1.2.1.1.97.100.109.105.110
- Password: 1.3.6.1.4.1.4684.2.17.1.1.1.2.97.100.109.105.110
- WEP Keys Index: 1.3.6.1.4.1.4684.2.14.2.5.1.2
- WPA PSK: 1.3.6.1.4.1.4491.2.4.1.1.6.2.2.1.5.6
- SSID: 1.3.6.1.4.1.4684.2.14.1.2.0

DDW3611

- 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

SNMP is not enabled by default on these devices, blogged Heiland. However, a number of cable providers that utilize Ubee devices enable SNMP with the community string of "public" on the uplink side of the cable modem for remote

Flaws Allowing DoS Of Systems Using SNMP



http://www.squid-cache.org/Advisories/SQUID-2014_3.txt

Squid Proxy Cache Security Update Advisory SQUID-2014:3

Advisory ID: SQUID-2014:3
Date: September 15, 2014
Summary: Buffer overflow in SNMP processing
Affected versions: Squid 3.x -> 3.4.7
Fixed in version: Squid 3.4.8

---

http://www.squid-cache.org/Advisories/SQUID-2014_3.txt
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6270

Problem Description:

Due to incorrect buffer management Squid can be caused by an attacker to write outside its allocated SNMP buffer.

Severity:

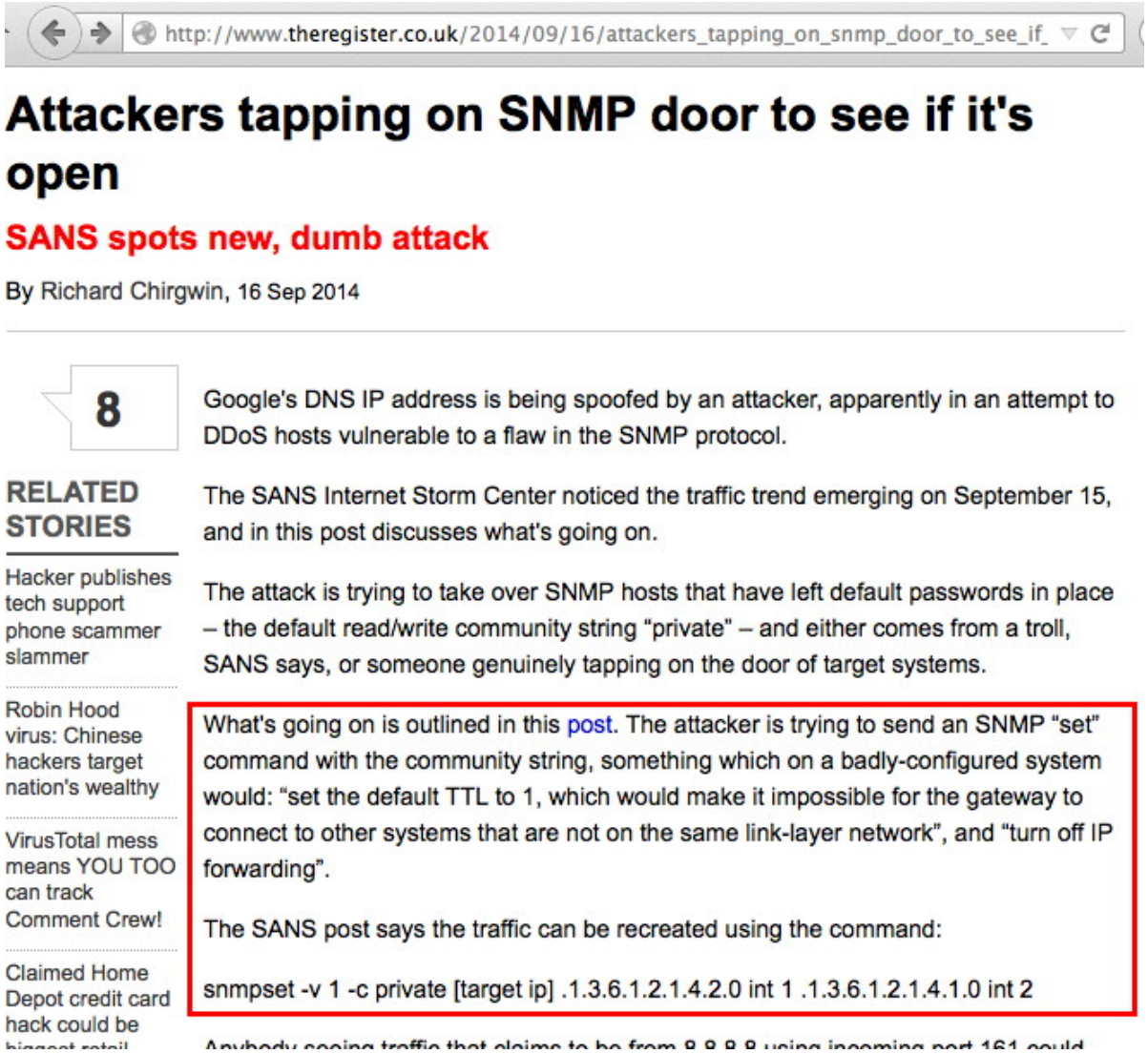
The bug is important because it allows remote attackers to crash Squid, causing a disruption in service. However, the bug is exploitable only if you have configured Squid to receive SNMP messages.

Sites that do not use SNMP are not vulnerable.

Updated Packages:

This bug is fixed by Squid version 3.4.8

SNMP-Based Forwarding Attack Attempt: Set TTL=1 and Disable IP Forwarding



http://www.theregister.co.uk/2014/09/16/attackers_tapping_on_snmp_door_to_see_if_

Attackers tapping on SNMP door to see if it's open

SANS spots new, dumb attack

By Richard Chirgwin, 16 Sep 2014

8

Google's DNS IP address is being spoofed by an attacker, apparently in an attempt to DDoS hosts vulnerable to a flaw in the SNMP protocol.

The SANS Internet Storm Center noticed the traffic trend emerging on September 15, and in this post discusses what's going on.

The attack is trying to take over SNMP hosts that have left default passwords in place – the default read/write community string "private" – and either comes from a troll, SANS says, or someone genuinely tapping on the door of target systems.

What's going on is outlined in this post. The attacker is trying to send an SNMP "set" command with the community string, something which on a badly-configured system would: "set the default TTL to 1, which would make it impossible for the gateway to connect to other systems that are not on the same link-layer network", and "turn off IP forwarding".

The SANS post says the traffic can be recreated using the command:

snmpset -v 1 -c private [target ip] .1.3.6.1.2.1.4.2.0 int 1 .1.3.6.1.2.1.4.1.0 int 2

RELATED STORIES

Hacker publishes tech support phone scammer slammer

Robin Hood virus: Chinese hackers target nation's wealthy

VirusTotal mess means YOU TOO can track Comment Crew!

Claimed Home Depot credit card hack could be

There Are MANY Other Problems with SNMP

- A year or two ago I warned you that there were MANY problems with SSL/TLS, and I told you that people weren't correctly configuring SSL/TLS. [I'm talking more about that here tomorrow at 8:30AM] Since then, SOME of those SSL/TLS problems have surfaced in the form of things like Heartbleed, Poodle, etc.

- **Today I'm raising a similar red flag about SNMP**. We all really need to be paying attention to this protocol. We also need to be working as a community to fix its protocol-level issues, and to clean up how it's been deployed to-date.

- And yes, we need to pay attention to SNMP's crypto, too.

Section 2. SNMP's Crypto

NO Crypto Support (In Early Versions)

- Because SNMP is a very old protocol, and because SNMP also needed to be usable even on very simple/low horsepower devices, it historically did not support encryption.

- Unencrypted SNMP connections represent an obvious problem when you realize that SNMP authentication protocols are quite "basic", and readily vulnerable to **sniffing** over the wire

- Things are particularly bad if SNMP protocols are routinely used for configuration management purposes, e.g., "set" (or "write") access rather than just "get" (or "read") access

An SNMP Encryption Support Summary

- SNMP v1: **NO CRYPTO, DON'T USE**
- SNMP v2c: **NO CRYPTO, DON'T USE**
- **SNMP v3: LIMITED CRYPTO SUPPORT**

- What does "LIMITED" mean?

- To be blunt, SNMP crypto support lags far behind what's available for https.

MD-5/SHA-1/SHA-2

- One example of the primitive state of SNMP crypto is easy to identify: as soon as you begin looking at SNMP, you see references to MD-5 and SHA-1 for SNMP authentication. Ugh.

- Good news (since most of the world is busily phasing out SHA-1): SNMP SHA-2 protocol support is being worked on, see:

  "HMAC-SHA-2 Authentication Protocols in USM for SNMP draft-hmac-sha-2-usm-snmp-01," http://tools.ietf.org/html/draft-hmac-sha-2-usm-snmp-01 (Expires November 7th, 2014)

Symmetric Cipher Suites: More Crypto Trouble?

- Implementations of SNMP v3 often do DES (see "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)," https://tools.ietf.org/html/rfc3414).
- **DES is NOT cryptographically adequate** (see the next slide).
- Things got better with support for **AES-128** per "The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model," http://tools.ietf.org/html/rfc3826
- In a limited number of even MORE uncommon cases, you'll even have support for **AES-256**, which is excellent (this is typically via vendor SNMP extensions)
- Unfortunately, we need strong crypto for ALL SNMP devices, not just for rare exceptions.

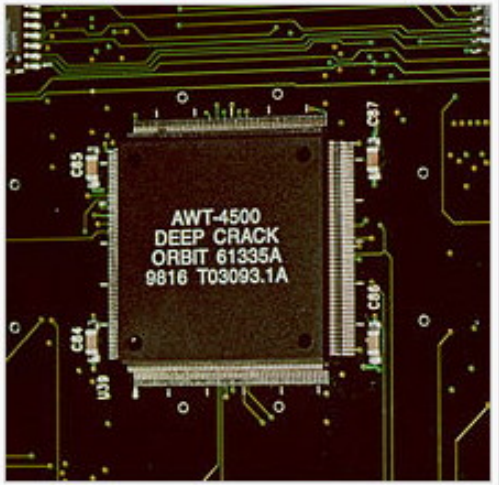
The Problem with DES As A Crypto Option...

/en.wikipedia.org/wiki/EFF_DES_cracker

snmp v2c encryption

nks

In 1998, the EFF built Deep Crack for less than $250,000.[3] In response to DES Challenge II-2, on July 15, 1998, Deep Crack decrypted a DES-encrypted message after only 56 hours of work, winning $10,000. This was the final blow to DES, against which there were already some published cryptanalytic attacks. [citation needed] The brute force attack showed that cracking DES was actually a very practical proposition. For most governments or large corporations, building a machine like Deep Crack would pose few problems.



The EFF's DES cracker "Deep Crack" custom microchip.

Six months later, in response to RSA Security's DES Challenge III, and in collaboration with distributed.net, the EFF used Deep Crack to decrypt another DES-encrypted message, winning another $10,000. This time, the operation took less than a day — 22 hours and 15 minutes. The decryption was completed on January 19, 1999. In October of that year, DES was reaffirmed as a federal standard, but this time the standard recommended Triple DES.

The small key-space of DES, and relatively high computational costs of Triple DES resulted in its replacement by AES as a Federal standard, effective May 26, 2002.

One Vendor's AES-128 Support

Configuring the Advanced Encryption Standard Algorithm

To configure the Advanced Encryption Standard (AES) algorithm for an SNMPv3 user, include the `privacy-aes128` statement at the `[edit snmp v3 usm local-engine user username]` hierarchy level:

```
[edit snmp v3 usm local-engine user username]
privacy-aes128 {
    privacy-password privacy-password;
}
```

privacy-password is the password used to generate the key used for encryption.

SNMPv3 has special requirements when you create plain-text passwords on a router or switch:

- The password must be at least eight characters long.
- The password can include alphabetic, numeric, and special characters, but it cannot include control characters.

Source: http://www.juniper.net/techpubs/en_US/junos14.1/topics/task/configuration/snmpv3-encrypton-type-configuring-junos-nm.html

AES-256 Support From Another Vendor

Encryption Key Support

In the AES and 3-DES Encryption Support for SNMP Version 3 feature the Cipher Block Chaining/Data Encryption Standard (CBC-DES) is the privacy protocol. Originally only DES was supported (as per RFC 3414). This feature adds support for AES-128 (as per RFC 3826) and AES-192, AES-256 and 3-DES (as per CISCO-SNMP-USM-OIDS-MIB).

- AES encryption uses the Cipher Feedback (CFB) mode with encryption key sizes of 128, 192, or 256 bits.
- 3DES encryption uses the 168-bit key size for encryption.

The AES Cipher Algorithm in the SNMP User-based Security Model draft describes the use of AES with 128-bit key size. However, the other options are also implemented with the extension to use the USM. There is currently no standard for generating localized keys for 192- or 256-bit size keys for AES or for 168-bit size key for 3-DES. There is no authentication protocol available with longer keys.

Management Information Base Support

The AES and 3-DES Encryption Support for SNMP Version 3 feature supports the selection of privacy protocols through the CLI and the Management Information Base (MIB). A new standard MIB, SNMP-USM-AES-MIB, provides support for the 128-bit key in AES. The extended options of AES with 192- or 256-bit keys and 3-DES are supported as extensions to the SNMP-USM-MIB, in the Cisco-specific MIB, CISCO-SNMP-USM-EXT-MIB.

See http://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t2/snmpv3ae.html

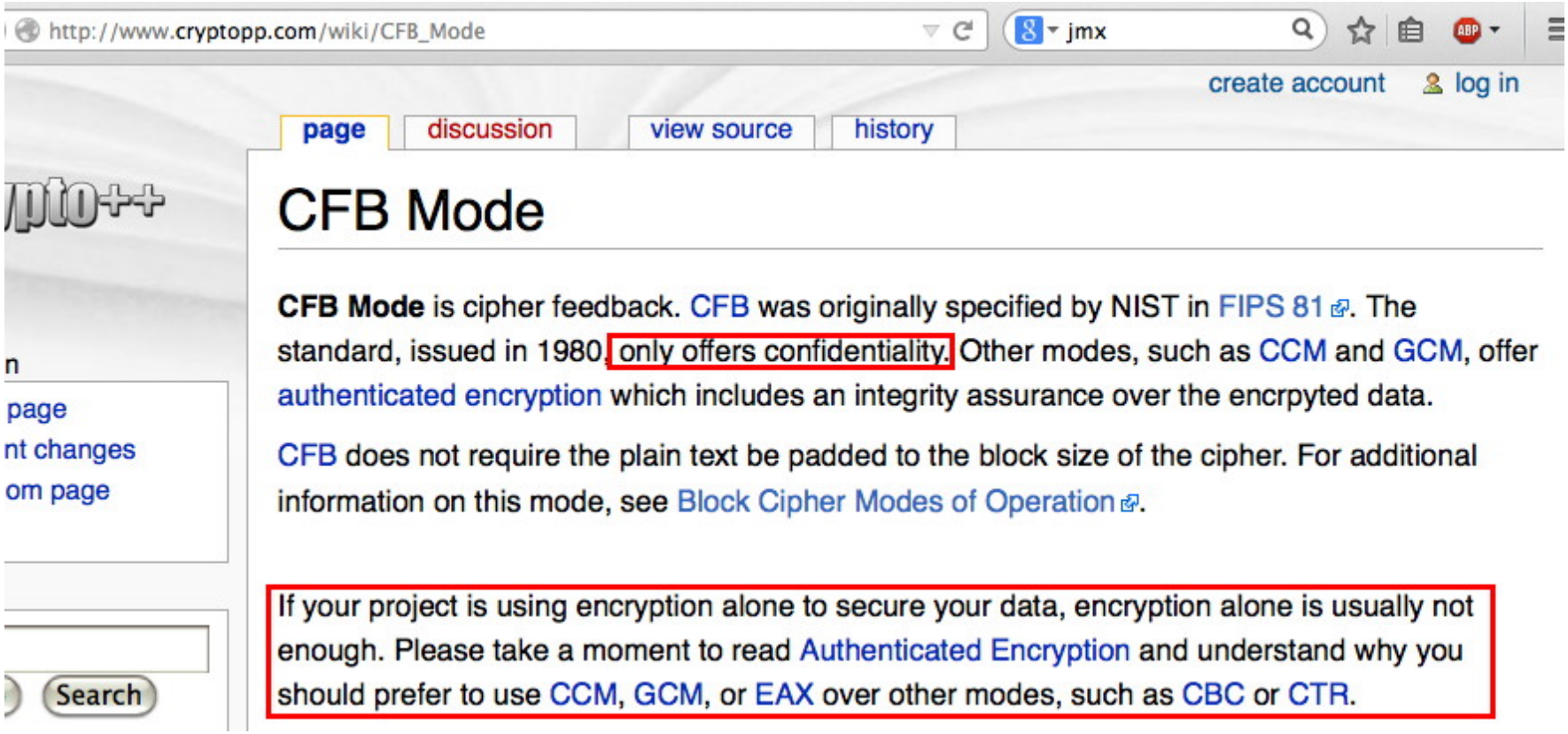
AES in *CFB* Mode?

- http://www.ietf.org/rfc/rfc3826.txt at 3.1.1.1 ("Mode of operation") says:

  "The NIST Special Publication 800-38A [AES-MODE] recommends five confidentiality modes of operation for use with AES: Electronic Codebook (ECB), Cipher Block Chaining (CBC), ***Cipher Feedback (CFB)***, Output Feedback (OFB), and Counter (CTR). ***The symmetric encryption protocol described in this memo uses AES in CFB mode*** *with the parameter S (number of bits fed back) set to 128 according to the definition of CFB mode given in [AES-MODE]. This mode requires an Initialization Vector (IV) that is the same size as the block size of the cipher algorithm."*

  CFB is a relatively uncommon mode.

What Does the Crypto Community Say?



Recap: What Crypto Work Might SNMP Need?

- We need to begin treating SNMP crypto as if it is **JUST as critical as https crypto, if not more.** We need it to be closely scrutinized, and we probably need automated tools like the Qualys SSL Tester but for SNMP crypto.
- SNMP needs standardized SHA-2 support.
- SNMP support for AES-256 should be ubiquitous.
- Do we need a hard look at the decision to use CFB mode with AES? Are the initialization vectors (IV) appropriately?
- Is there/should there be any worry about MITM risks for SNMP? That is, how do you know you're providing your credentials to the "right" SNMP-using device currently?
- What about low end (low horsepower) systems that need to do SNMP? Will they be okay with moving to beefier crypto?

Section 3. Community Strings

Default Passwords Are A Well Known Threat

- Pen testers (as well as less benign individuals) are well aware that default passwords often get configured "at the factory" and then are forgotten/never changed.

- There are many lists of default device passwords in circulation, including (among others):

  -- http://www.defaultpassword.com/
  -- http://www.routerpasswords.com/

- SNMP has its own version of the "default password problem," namely **default community strings**.

Default Community Strings

- If your device has a **read** community string of

  public

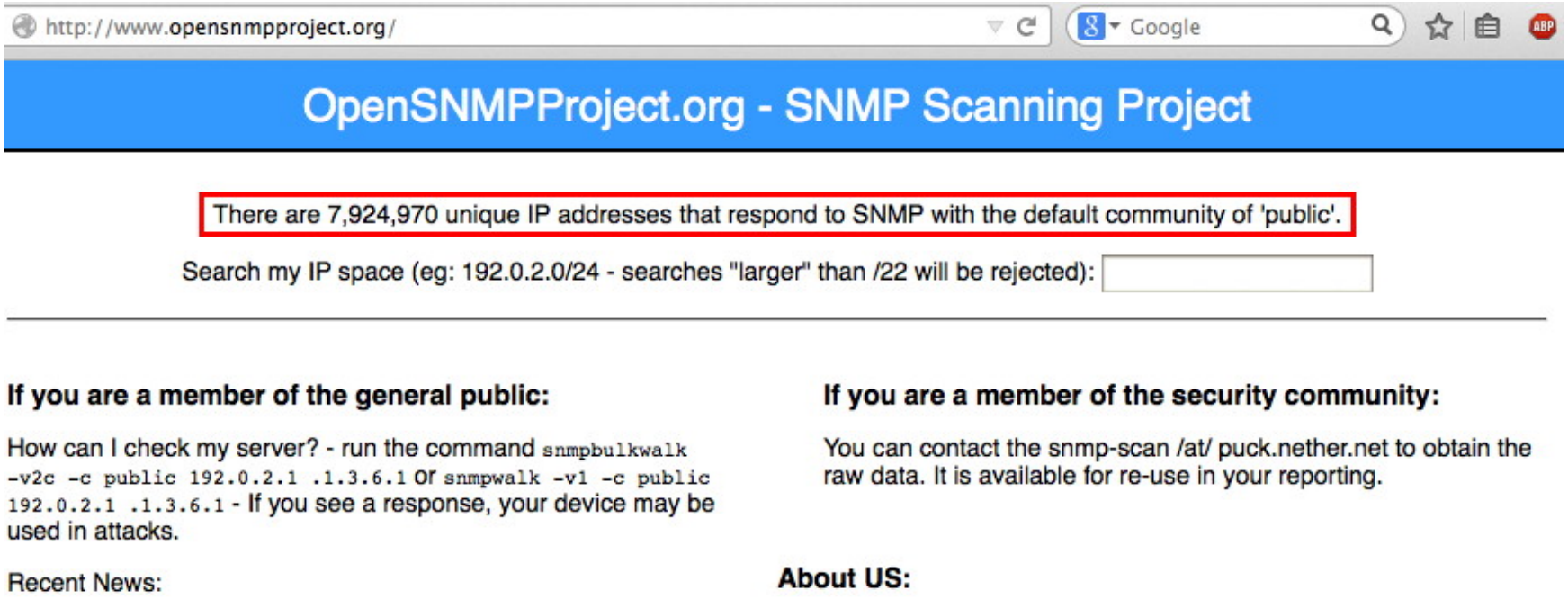
  or a **write** community string of

  private

  you're either running a honeypot or **you're crazy.**

- If you're using one of the other common SNMP community strings listed at https://code.google.com/p/fuzzdb/source/browse/trunk/wordlists-misc/wordlist-common-snmp-community-strings.txt you're just about **equally as nuts.**

There Are A LOT of Crazy People Out There



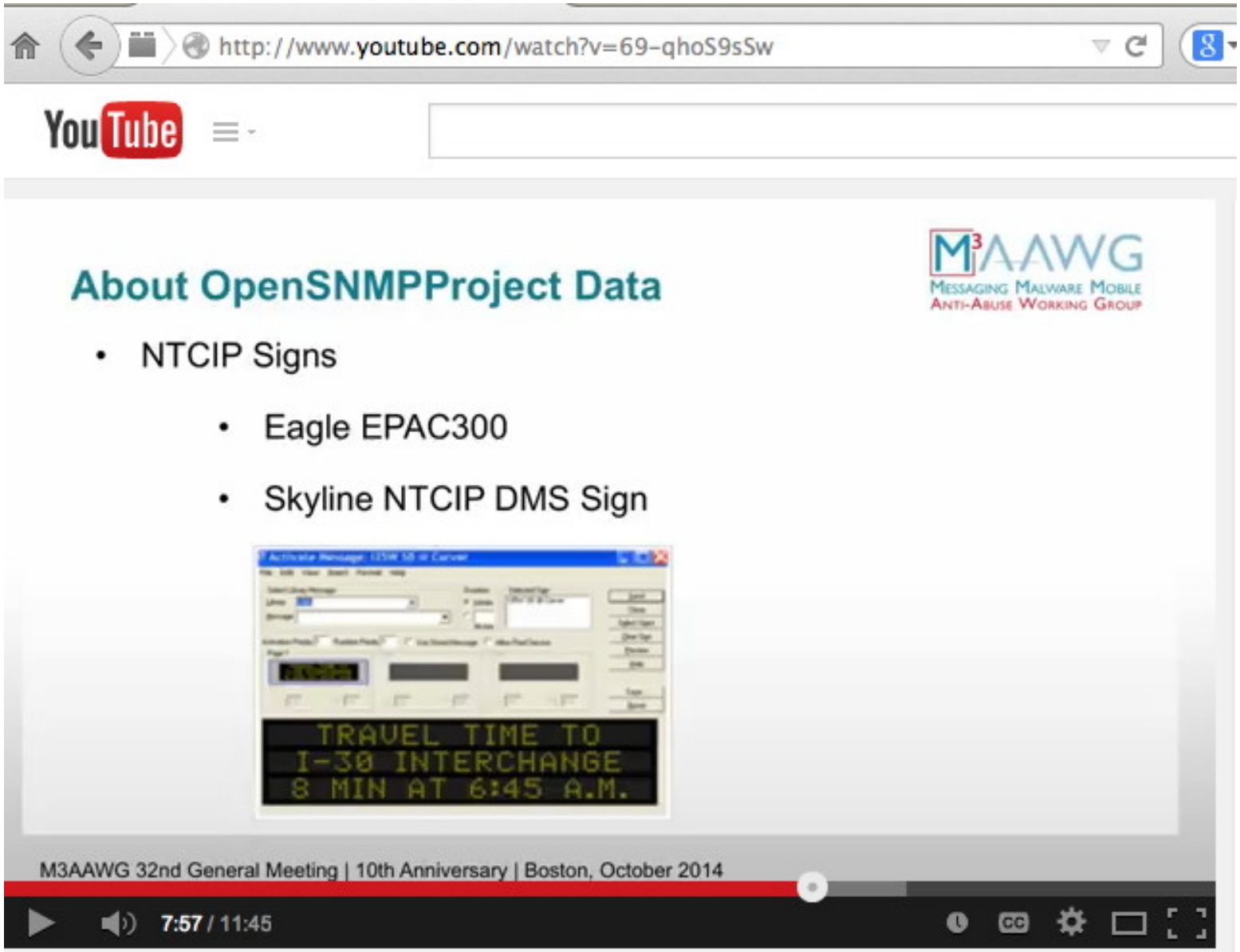
Jared Just Won The JD Falk Award For His Work

October 21, 2014 14:50 ET

Open Resolver Project Founder Jared Mauch Receives M3AAWG J.D. Falk Award for Identifying Systems at Risk

BOSTON, MA--(Marketwired - Oct 21, 2014) - ***M^{3}AAWG General Meeting*** -- The founder of a far-reaching, volunteer program to identify millions of servers on the Internet with open DNS settings that could be commandeered in DDoS and spoofing attacks was honored with the 2014 J.D. Falk Award at the M^{3}AAWG 32nd General Meeting today in Boston. Jared Mauch received the award from the Messaging, Malware and Mobile Anti-Abuse Working Group for three related projects that help prevent vulnerable servers from being used in cyber assaults: The Open Resolver Project, the Open NTP Project and the Open SNMP Project.

With the frequency and intensity of DDoS attacks escalating, pinpointing the enormous number of Internet-facing servers with open DNS and other network settings that can be unknowingly deployed in these outbreaks is an important but massive undertaking. The programs developed by Mauch collect current Internet data to identify exposed machines and provide this information to the trusted security community for remediation.



Jared Mauch Receives J.D. Falk Award for Open Resolver Project

The SAME Community Strings on ALL Devices?

- Let's assume that you're NOT crazy, and you've set a non-default / uncommon community string for read and write access.

- Did you set the SAME community string for ALL managed devices on your campus? Are all those devices of equal sensitivity/importance?

- Don't we routinely preach at users about the risks of using the same passwords on multiple systems?

- Yes, I know that having unique per-device SNMP communities "adds complexity" or "is impractical" when teams manage large networks, but...

What About Brute Force Attacks on SNMP?

- Are you paying attention to potential brute force attacks against your community strings? SNMP brute forcing/dictionary attack tools are widely available:

  -- http://nmap.org/nsedoc/scripts/snmp-brute.html
  -- https://www.thc.org/thc-hydra/
  -- etc., etc., etc.

  You can probably arrange to monitor SNMP traps for failed password attempts, if you're into whack-a-moling.

- Of course, random people shouldn't have access to SNMP on your managed devices in the first place, now should they?

When Did You Last CHANGE Your Device Community String(s)?

- For example:

  -- If one or more **staff have left**, did you change any community strings that they may have known?

  -- If you've used the same community strings for the last year, do you think it might be time to schedule a network wide change?

  -- What does your school's policies say? What do your auditors expect? Have they ever ***asked*** about your community strings? Should your SNMP practices be something that they DO ask about/look at?

Something Better Than Plain Old Passwords?

- And it sure would be nice if SNMP could also do some sort of strong authentication (should as client certificates on smartcards), at least if you're modifying meaningful systems via SNMP.

Section 4. Limiting Network Access To SNMP

"First Of All, Do I Need To Run SNMP At All?"

- If you don't need to run SNMP, **DON'T.** (Disabling unneeded services is the best way to reduce your attack surface.)

- However, disabling SNMP is a strategy that comes at the cost of substantial collateral damage. Taken to an extreme, totally blocking SNMP access might mean that you're suddenly having to try to run a large network more or less totally blind. That's going too far.

- You're probably better off just heavily "fencing SNMP in."

- Sadly, at least some people **DON'T** bother limiting access to SNMP.

The Basic: Block Port 161 and 162 At The Border

- I'm not a huge fan of port-based blocks, but there shouldn't be **ANY** port 161 (SNMP) nor ANY port 162 (SNMP Trap) traffic crossing your campus border inbound OR outbound

  Be sure you block 161 an 162 on both IPv4 **AND IPv6** (assuming your network supports both IPv4 and IPv6)

- One example of a campus that currently blocks 161 and 162:

  http://www.net.princeton.edu/filters/internet-border.html

  Good job, Princeton! A+

SNMP Doesn't ONLY Run Over Port 161 and 162

On November 28, 2012, US-CERT issued an advisory warning that select Samsung/Dell printers contained a hardcoded backdoor that could be accessed via SNMP. There are a lot of interesting facts surrounding this vulnerability, including:

- The backdoor SNMP service listens on a non-standard UDP port 1118
- The password for the backdoor is "s!a@m#n$p%c" and allows both SNMP reads and writes. This allows an attacker to change the configuration settings, including resetting the username/password to the device to gain full administrative access
- Researchers report firmware dating back to 2004 contains this same password for the SNMP community string
- If SNMP is disabled on the printer, it does not remove the SNMP backdoor on port 1118
- Before the vulnerability went public, Samsung pulled all the printer firmware from their download sites
- Dell printer firmware remains on Dell's website for download.

We Empirically Know Some Sites Do NOT Bother Blocking Port 161 At The Border, Anyhow

- If you'd like to see the problem first hand, **create a free Shodan account** (http://www.shodanhq.com/), then do a query for

  hostname:.edu port:161

- **When I did this query on the 28th of October, 2014, Shodan found 30,256 matching edu hosts in the US. (NOT good)**

- If you get a Shodan account and run a report on that query, you can see the responsible organizations. **Just four (4) US universities accounted for over half of those accessible SNMP hosts; fix those four sites and roughly 17,000 problematic hosts go away. Is YOUR campus one of those sites?**

So What *IS* Shodan Finding and Reporting?

- If you want to see those four campuses, you'll have to check for yourself.

- However, reportedly the top product seen by Shodan was the **"Symbol Spectrum Access Point,"** a wireless access point. This product was seen at a level that was more than 2X the next most common SNMP-able device in higher education.

- The report also identified Linux 2.6.x (believed in this case to be showing up because of its use in things like networked printers), and Windows 7 or 8, plus **Windows XP**, among others. Note, of course, that Windows XP is end-of-life, and really shouldn't be getting seen on the wire AT ALL (much less doing SNMP!) Has YOUR campus phased out Windows XP? If not, why not?

Internally Control Network SNMP Traffic, Too

- **Scenario*: "What if an intruder compromises a system that's inside the perimeter? They can then use that host as a stepping stone for SNMP attacks!"***

- One option for limiting opportunities for SNMP-related mischief on campus is to run a **separate out-of-band network** reserved exclusively for all SNMP traffic.

- If that's not "practical," you may at least want to consider restrictions on where SNMP traffic can flow internally. That is, if all your network management work is done from one dedicated network engineering subnet, why allow SNMP traffic from the campus wireless network, or your residence hall network, etc.?

BCP 38/BCP 84

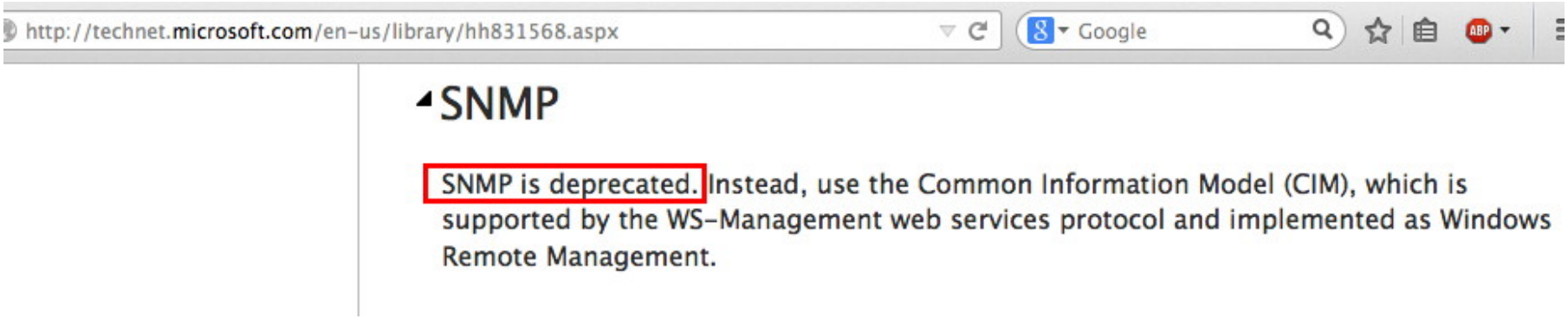
- In addition to blocking SNMP specifically, you should ALSO be taking steps to block packets with spoofed source addresses from leaving your network. For example, at UO, where packets should be coming from 128.223.0.0/16, packets that pretend to come from some other source IP address should be dropped.

- Spoofed traffic is one of the crucial elements that make reflective amplification attacks of ALL types possible. Block spoofed traffic, please!

- See:

  -- http://tools.ietf.org/html/bcp38 and
  -- http://tools.ietf.org/html/bcp84

SNMP's Days May Be Getting Short(er)



Source: "Features Removed or Deprecated in Windows Server 2012," http://technet.microsoft.com/en-us/library/hh831568.aspx

Note carefully: "deprecated" is NOT synonymous with "removed!" SNMP may still be present and used on Windows Server 2012!

[BTW, if curious about CIM, see http://en.wikipedia.org/wiki/Common_Information_Model_%28computing%29]

Section 5. Conclusion

The One Slide Summary Message

- SNMP is everywhere, and it can be grossly insecure; it's on the smallest and largest hosts, and it's used in control systems, too
- SNMP can hurt you, and *others,* if not carefully limited
- Disable it if you don't need it or you're not actively using it
- If you must run it, run SNMPv3 only, NOT SNMP v1 NOR v2c
- Don't use stupid default community strings like "public"!
- Use SHA-1 if your device supports it, NOT MD5! Push your vendors to phase in SHA-2!
- Use AES-128 or AES-256 if your device supports it; if your device doesn't support it, bug your vendor. Don't trust DES!
- **BLOCK port 161 and 162 at your border!**
- **Implement BCP38/BCP84 anti-spoofing filters at your border, too!**

A Personal Note

- I'll be concluding my work with Internet2 and InCommon and the University of Oregon at the end of the month to take a new position with Paul Vixie's data-driven security company Farsight Security (https://www.farsightsecurity.com/)

- It's been a real honor and privilege to have had the chance to work with all of you, and I particularly appreciate your putting up with me preaching at you about security issues – especially if you're at a school that's already proactively doing the right thing.

- Copies of my talks will continue to be available from my personal web site, https://www.stsauver.com/joe/ and if you ever need to reach me, joe@stsauver.com should work.

Thanks For The Chance To Talk Today

- Are there any questions?

- Don't forget, there's another session I'll be doing, too, tomorrow morning at 8:30AM ("New Crypto 101")