# Abusing Software Defined Networks

DefCon 22, Las Vegas 2014

# Hellfire Security

Gregory Pickett, CISSP, GCIA, GPEN
Chicago, Illinois

gregory.pickett@hellfiresecurity.com

# Overview

- What is it?
- Exploiting it!
- Fixing it!
- Moving Forward
- Wrapping Up

# *Modern Day Networks*

- Vendor Dependent
- Difficult to scale
- Complex and Prone to Break
- Distributed and Often Inconsistent Configuration
- Uses inflexible and difficult to innovate protocols
- Unable to Consider Other Factors

… *And Good Luck If You Want To Change It!*

# *Enter . . . Software Defined Networking*

- Separate the Control and Data Plane
  - Forwarding Decisions Made By a Controller
  - Routers and Switches Just Forward Packets
- Controllers
  - Programmed with the Intelligence
  - Full visibility of the Network
  - Can consider the totality of the network before making any decision
  - Enforce Granular Policy

# Enter . . . Software Defined Networking

- Switches
  - Bare-Metal Only
  - Any Vendor … Hardware or Software

# Solves Lots of Problems

- Know the State of the Network Rather Than Inferring It
- Run Development and Production Side-By-Side
- More Practical …

# Solves Lots of Problems

- Less Expensive Hardware
- BGP
  - Maintenance Dry-Out
  - Customer Egress Selection
  - Better BGP Security
  - Faster Convergence
  - Granular Peering at IXPs

# Solves Lots of Problems

- Real-World Network Slicing of Flow Space
- Network and Server Load Balancing
- Security
  - Dynamic Access Control
  - Adaptive Traffic Monitoring
  - Attack Detection and Mitigation

# *Emerging Standards*

- Old and Busted
  - SNMP
  - BGP
  - Netconf
  - LISP
  - PCEP
- New Hotness
  - OVSDB
  - Openflow

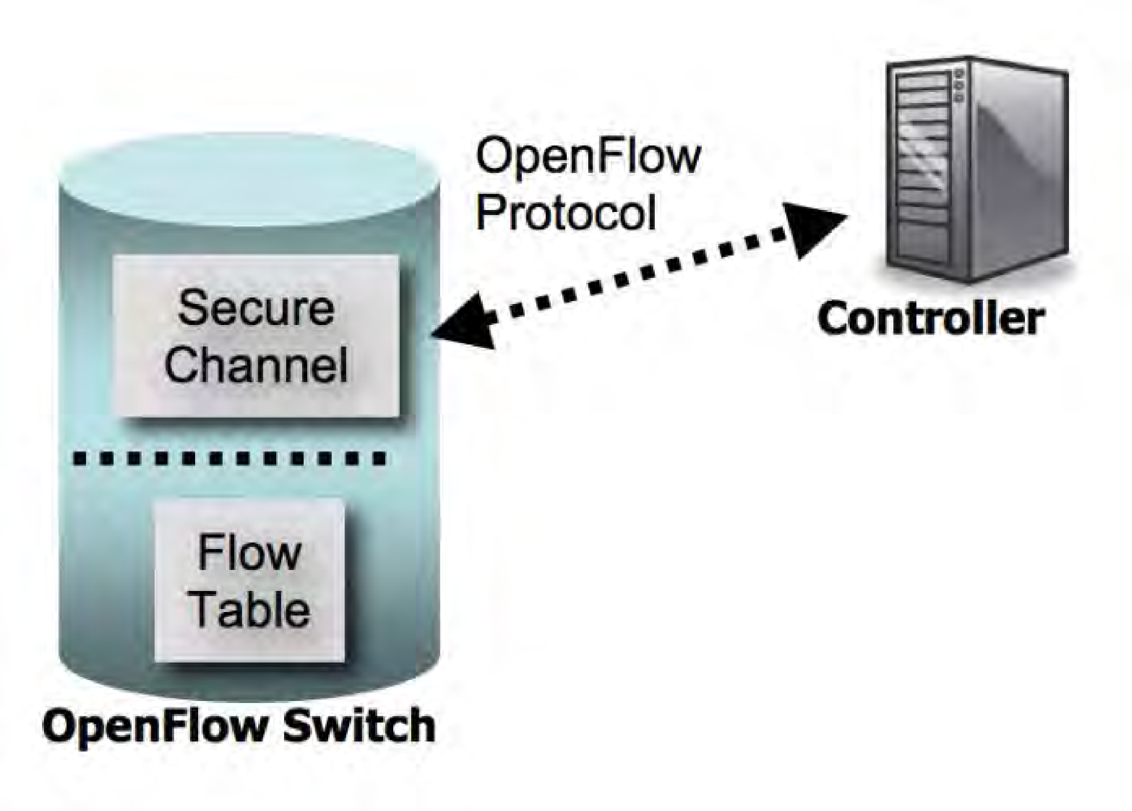
# *Introducing Openflow*

- Purpose
  - Execute Logic At the Controller
  - Update Forwarding Tables
- Defined
  - Forwarding Process
  - Messaging Format

# *Introducing Openflow*

- Elements
  - Controller
  - Secure Channel
  - Forwarding Element
- Process
  - Check Flow Table
  - If Match Found, Execute Action
  - If No Match, Send Packet to controller
  - Update Flow Table

# Introducing Openflow



# *Features*

- Flow Tables
  - Match/Action Entries
  - Packet header matched against 1 of N tables
  - 12 fields available for matching
  - Wildcard matching available
- Actions
  - Forward
  - Drop
  - Modify
  - Enqueue

# *Leading Platforms*

- Proprietary
  - Cisco Application Policy Infrastructure Controller (APIC)
  - Cisco Extensible Network Controller (XNC)
  - HP Virtual Application Networks (VAN) SDN Controller
  - IBM Programmable Network Controller
- Open-Source
  - Nox/Pox
  - Ryu
  - Floodlight
  - Opendaylight

# *Floodlight*

- Open-Source Java Controller
- Primarily an Openflow-based controller
- Supports Openflow v1.0.0
- Fork from the Beacon Java Openflow controller
- Maintained by Big Switch Networks

Project Floodlight

# *Opendaylight*

- Open-Source Java Controller
- Many southbound options including Openflow
- Supports Openflow v1.0.0 and v1.3.0
- Fork from the Beacon Java Openflow controller
- A Linux Foundation Collaborative Project
- Supported by Citrix, Red Hat, Ericsson, Hewlett Packard, Brocade, Cisco, Juniper, Microsoft, and IBM

OPEN
DAYLIGHT

# *How Prevalent Is It Going To Be?*

- Gartner: 10 critical IT trends for the next five years
- Major Networking Vendors Have Products or Products Planned for SDN
- InformationWeek 2013 Survey
  - 60% felt that SDN would be part of their network within 5 Years
  - 43% already have plans to put it in production

# So It's Gonna Be All . . .

## Not Exactly!

# Protocol Weaknesses

- Encryption and Authentication via TLS
- More of a suggestion than a requirement though …
  - Started Out Good
  - Heading Backwards
    - v1.0.0 over TLS
    - v1.4.0 over TCP or TLS

# *Protocol Weaknesses*

- Controllers
  - Floodlight … Nope
  - Opendaylight … Supported but not required
- Switches
  - Arista … No
  - Brocade … Surprisingly, Yes
  - Cisco … Another, Yes
  - Dell … No
  - Extreme … Another, Yes
  - HP … No

# Protocol Weaknesses

- Switches
  - Huawei … No
  - IBM … No
  - Juniper … No
  - NEC … Another, Yes
  - Netgear … No
  - Pronto … Yes
  - OVS … No

# Could Lead To . . .

- Information Disclosure through Interception
- Modification through Man-in-the-Middle
- And all sorts of DoS Nastiness!

# Debug Ports

- No Encryption
- No Authentication
- Just Full Control of the Switch
- All Via “dpctl” command-line tool

# Debug Ports

- Switches
  - Arista … Yes
  - Brocade … Yes
  - Dell … Yes
  - Extreme … Yes
  - HP … Yes
  - Huawei … Yes
  - IBM … Yes
  - Juniper … Yes
  - NEC … Yes

# Debug Ports

- Switches
  - Netgear … Yes
  - Pronto … Yes
  - OVS … Yes

# DoS Nastiness

- Openflow
  - Centralization Entails Dependency
  - Dependency Can Be Exploited
  - How are vendors handing it?
- Floodlight
  - Explored by Solomon, Francis, and Eitan
  - Their Results … Handling It Poorly
- Opendaylight
  - Unknown but worth investigating
  - It is Java for God Sake!

# Tools

- of-switch.py
  - Impersonates an Openflow switch
  - Utilizes Openflow v1.00
- of-flood.py
  - Floods an Openflow controller
  - Disrupting the network and bringing it down
  - Utilizes Openflow v1.00

# Demonstration

# Other Controller Weakness

- Floodlight
  - No Encryption for Northbound HTTP API
  - No Authentication for Northbound HTTP API
- Opendaylight
  - Encryption for Northbound HTTP API
    - Turned Off by Default
  - Authentication for Northbound HTTP API
    - HTTP Basic Authentication
    - Default Password Weak
    - Strong Passwords Turned Off by Default

Project Floodlight

OPEN DAYLIGHT

# *Could Lead To . . .*

- Information Disclosure through Interception
  - Topology
  - Credentials
- Information Disclosure through Unauthorized Access
  - Topology
  - Targets

Project Floodlight

OPEN DAYLIGHT

# *And . . .*

- Topology, Flow, and Message Modification through Unauthorized Access
  - Add Access
  - Remove Access
  - Hide Traffic
  - Change Traffic

Project Floodlight

OPEN DAYLIGHT

# *Identifying Controllers and Switches*

- Currently Listening on TCP Port 6633
- New Port Defined … TCP Port 6653
- Hello’s Exchanged
- Feature Request
  - Controller will send
  - Switch will not

Project Floodlight

OPEN DAYLIGHT

# Tools

- of-check.py
  - Identifies Openflow Services
  - Reports on their Versions
  - Compatible with any version of Openflow
- of-enum.py
  - Enumerates Openflow Endpoints
  - Reports on their Type
  - Compatible with any version of Openflow

# Tools

- openflow-enum.nse
  - Identifies Openflow Services
  - Reports on their Versions
  - Compatible with any version of Openflow

# Demonstration

# Exposure

- Number of Known Issues
- Bad Enough Inside a Network
- Is Anything Outward Facing?
- Better Not to Take Anyone’s Word for It
- Just Find Out for Yourself

# Reported

- While Data Centers/Clouds are the Killer App for SDN
  - NIPPON EXPRESS
  - FIDELITY INVESTMENTS
  - VMWARE
- Starting to see it moving toward the LAN
  - Caltech
  - Cern
- And WAN
  - Google, NTT, and AT&T

# Discovered (Scanning Project)

- Service Discovery Ran on Entire Internet
- Seeing Both Controllers and Switches
- Still Going Through Results Though
- Data Collected Full of Noise
- Let's Just Say that I Now Know Where All the Tarpits Are!

# Some Attacks

- Small Local Area Network
  - One Admin Host
  - Two User Hosts
  - One Server
  - One IDS
- Attacker will …
  - Identify Targets
  - Enumerate ACLs
  - Find Sensors

Project Floodlight

# Tool

- of-map.py
  - Downloads flows from an Openflow controller
  - Uses the flows
    - To identify targets and target services
    - To build ACLs
    - To identify sensors
  - Works with Floodlight and Opendaylight via JSON

# Demonstration

# And Some More Attacks . . .

- Small Local Area Network
  - One Admin Host
  - Two User Hosts
  - One Server
  - One IDS
- Attacker will …
  - Gain Access to the Server
  - Isolate the Administrator
  - Hide from the IDS
  - And Attack the Server

Project Floodlight

# Tool

- of-access.py
  - Modifies flows on the network through the Openflow Controller
    - Adds or Removes access for hosts
    - Applies transformations to their network activity
    - Hides activity from sensors
  - Works with Floodlight and Opendaylight via JSON

Project Floodlight

OPEN DAYLIGHT

# Demonstration

# And Some Pwnage . . .

Sorry Linux Foundation!

# Zero-Day Exploit

- Opendaylight has other southbound APIs besides Openflow
  - No Encryption for Southbound Netconf API
  - No Authentication for Southbound Netconf API
- Just Connect and Exchange Messages
  - XML-RPC
  - Remember Java?
- Boom Goes Opendaylight
- And it runs as “Root”

# Demonstration

# If No Exploit . . .

- Service Not Available or They Fix It
- Not to Worry
- Password Guess the !!!!!!
  - Default Password Weak
  - Strong Passwords Turned Off
  - No Account Lockout
  - No SYSLOG Output

OPEN DAYLIGHT

# Repeat!

- Attacker will …
  - Identify Targets
  - Enumerate ACLs
  - Find Sensors
  - Gain Access to the Server
  - Isolate the Administrator
  - Hide from the IDS
  - And Attack the Server
- And Pwn That Network Too!

OPEN
DAYLIGHT

# Demonstration

# Other Exploits Waiting to Be Found!

- Floodlight
  - Northbound HTTP API
  - Southbound Openflow API
- Opendaylight
  - Northbound HTTP API
  - Southbound Openflow API
  - Southbound Netconf API (TCP,SSH)
  - Southbound Netconf Debug Port

Project Floodlight

OPEN DAYLIGHT

# Other Exploits Waiting to Be Found!

- Opendaylight
  - JMX Access
  - OSGi Console
  - Lisp Flow Mapping
  - ODL Internal Clustering RPC
  - ODL Clustering
  - Java Debug Access

Project Floodlight

OPEN DAYLIGHT

# Where to Look

- Identify Additional Encryption and Authentication Issues
- Use Them to Explore
  - Direct Access
  - Traditional Vulnerabilities
- Start with the Basics
  - Protocol Messaging
  - Injection for RFI/LFI, Etc.
- Identify
  - Information Disclosure
  - Unauthorized Access
  - DoS

Project Floodlight

OPEN DAYLIGHT

# Available Solutions

- For Now
- For the Future

# *For Now*

- Transport Layer Security
  - Feasible?
  - Realistic?
- Hardening … Duh!
- VLAN … It’s the Network Stupid!
- Code Review Anyone?

# *For the Future*

- Denial of Service (SDN Architecture)
  - Network Partitioning
  - Controller Clustering
  - Static Flow Entries
- Modification (SDN Applications)
  - Traffic Counters
  - Respond to Abnormalities
- Verification (SDN Operations)

# *Impact*

- With this one box, you get everything they have
- There is the Obvious
  - Own Any Data They Own
  - Control Any Aspect of Their Operation
  - Control Their Fate
- Opens Up A World of Possibilities

# *How It Could Go Right*

- Vendor Independence and ultimately lower cost
- Networks that match the application and the businesses needs not the other way around
- Faster Evolution of the Network
  - Production-Scale Simulation and Experimentation
  - Exchangeable Network Aspects
- Dynamic and Truly Active Defenses

# *How It Could Go Wrong*

- Denial of Service
  - Peer Node
  - External Node
  - Selectively Dropping Traffic?
- MiTM
  - Entire Networks
  - Local Subnets or Hosts
- Shadow Operations
  - Darknets
  - Uber Admins

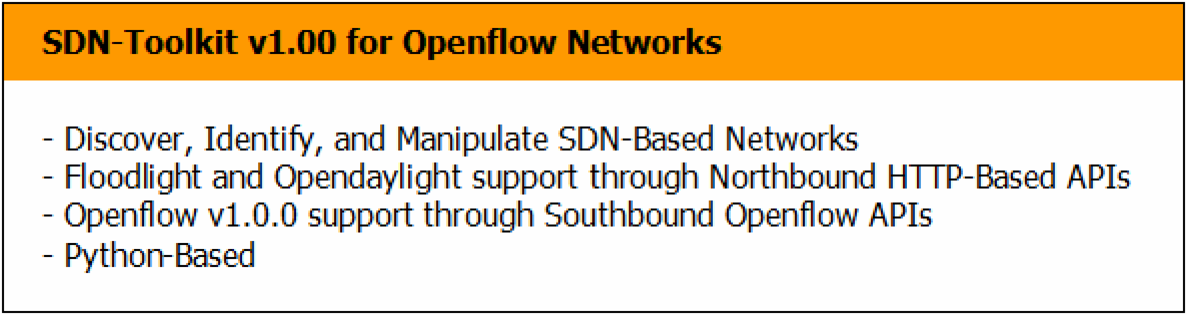
# *Making the Difference*

- Traditional Means of Securing Controllers Still Apply
- Security Needs to Be Part of the Discussion
  - Until Now … How SDN Can Help Security
  - But How Secure is SDN?
- Analyses being Done
  - But By Outsiders
  - Traditional Approach and 2-D
- Controller's Need A Security Reference and Audit Capability

# *Final Thoughts*

- SDN has the potential to turn the entire Internet into a cloud
- Benefit would be orders of magnitude above what we see now
- But there is hole in the middle of it that could easily be filled by the likes of the NSA … or worse yet, China
- Let’s Not Let That Happen
- And That Start’s Here

# Toolkit



**SDN-Toolkit v1.00 for Openflow Networks**

- Discover, Identify, and Manipulate SDN-Based Networks
- Floodlight and Opendaylight support through Northbound HTTP-Based APIs
- Openflow v1.0.0 support through Southbound Openflow APIs
- Python-Based

Updates can be found at http://sdn-toolkit.sourceforge.net/

# Links

- http://www.sdncentral.com/
- https://www.opennetworking.org/
- http://www.projectfloodlight.org/
- http://www.opendaylight.org/
- https://www.coursera.org/course/sdn
- https://www.baycollege.edu/Academics/Areas-of-Study/Computer-Network-Systems/Faculty/Linderoth/2013-sdn-survey-growing-pains.aspx
- http://www8.hp.com/h20195/v2/GetDocument.aspx?docname=4AA4-7944ENW
- http://www.openflowhub.org/blog/blog/2012/12/03/sdn-use-case-multipath-tcp-at-caltech-and-cern/
- http://www.networkworld.com/article/2167166/cloud-computing/vmware--we-re-building-one-of-the-biggest-sdn-deployments-in-the-industry.html
- http://www.networkcomputing.com/networking/inside-googles-software-defined-network/a/d-id/1234201?
- http://cseweb.ucsd.edu/~vahdat/papers/b4-sigcomm13.pdf
- http://viodi.com/2014/03/15/ntt-com-leads-all-network-providers-in-deployment-of-sdnopenflow-nfv-coming-soon/

# Q&A