NETCONF in the Wild

John Kristoff, jtk@[cymru.com,depaul.edu]
James Schaefer, jschaefe@depaul.edu
Maciej Leja, mleja2@depaul.edu

NETCONF on JUNOS

```
system {
   services {
      netconf {
         ssh {
            connection-limit limit;
            /* NOTE: default port is 830 */
            port port;
            rate-limit limit;
         }
      }
   }
}
```

Team Cymru
Secure JUNOS Template
Version 1.92, 03/30/2005

```
firewall {
    ...
    filter router-protect {
    . . .
                protocol tcp;
                destination-port ssh;
    ...
}
```

NETCONF didn't exist then. We are woefully out of date.
Help us?

What is out there?

- ~10 million random IPv4 NETCONF over SSH probes
  - Very few random port 830 NETCONF listeners
- ~6700 JUNOS Internet devices
  - Not enormous, but notable (dozens)
  - Includes some SSH < version 2
- ~10 million random IPv4 NETCONF over TLS probes
  - A small handful, but interesting listeners on 6513

Banner Fun

```
**************************************************************
*                                                            *
*                          WARNING!!!!!                      *
*                                                            *
*  This system is restricted to AT&T Mobility                *
*          authorized users for business purposes.           *
*                                                            *
*     Unauthorized access is a violation of the law.         *
*   This service may be monitored for administrative         *
*                   and security reasons.                    *
*    By proceeding, you consent to this monitoring.          *
*                                                            *
*                          WARNING!!!!!                      *
*                                                            *
**************************************************************
```

Certificate Fun

```
O: Jackson National Life Insurance Company

O: Beijing Topsec Network Security Technology
Co., Ltd.

O: HTTPS Management Certificate for SonicWALL
(self-signed)

O: securelogin.arubanetworks.com

CN: trade.stocktrade.co.uk

CN: v1.jdi.socom.mil
```

Threat Summary

- SSH service exposure
  - SSH version leak (correlates to JUNOS version)
  - SSH connection-limit DoS
  - SSH password authentication brute force attacks
  - SSH public key collection?
- TLS service exposure
  - X.509 certificate and system detail leak
  - Missing client authentication mechanisms?

Follow Up Work and Questions

- Investigate TLS threat landscape more fully
- How much Cisco NETCONF over SSH is out there?
- Does any use NETCONF over BEEP (831)?
- Would an ongoing IP address feed be helpful?
- Would a SSH keys and X.509 certs repo be useful?
- How dangerous might this be really?
- Education and vendor alert campaign needed?