Embedded Many-bit Linux

Quick Primer on Linux Security

Zak Estrada

ROSE-HULMAN INSTITUTE OF TECHNOLOGY

Is this a critical system?

Embedded device security is a big deal

- Embedded systems are often found in critical systems

- Cyber-physical systems
  - Power infrastructure
  - Medical devices
  - Cars

- Embedded devices typically use low-level interfaces
  - Lots of security issues there

Your BeagleBone was designed for ease of use

- “Security comes later”
  - Example: no root password by default!

- If you put it on the internet, it becomes an easy target

- Set a root password
- Only use root/sudo when needed
  - Create users/groups otherwise

ROSE-HULMAN INSTITUTE OF TECHNOLOGY

Principle of Least Privilege

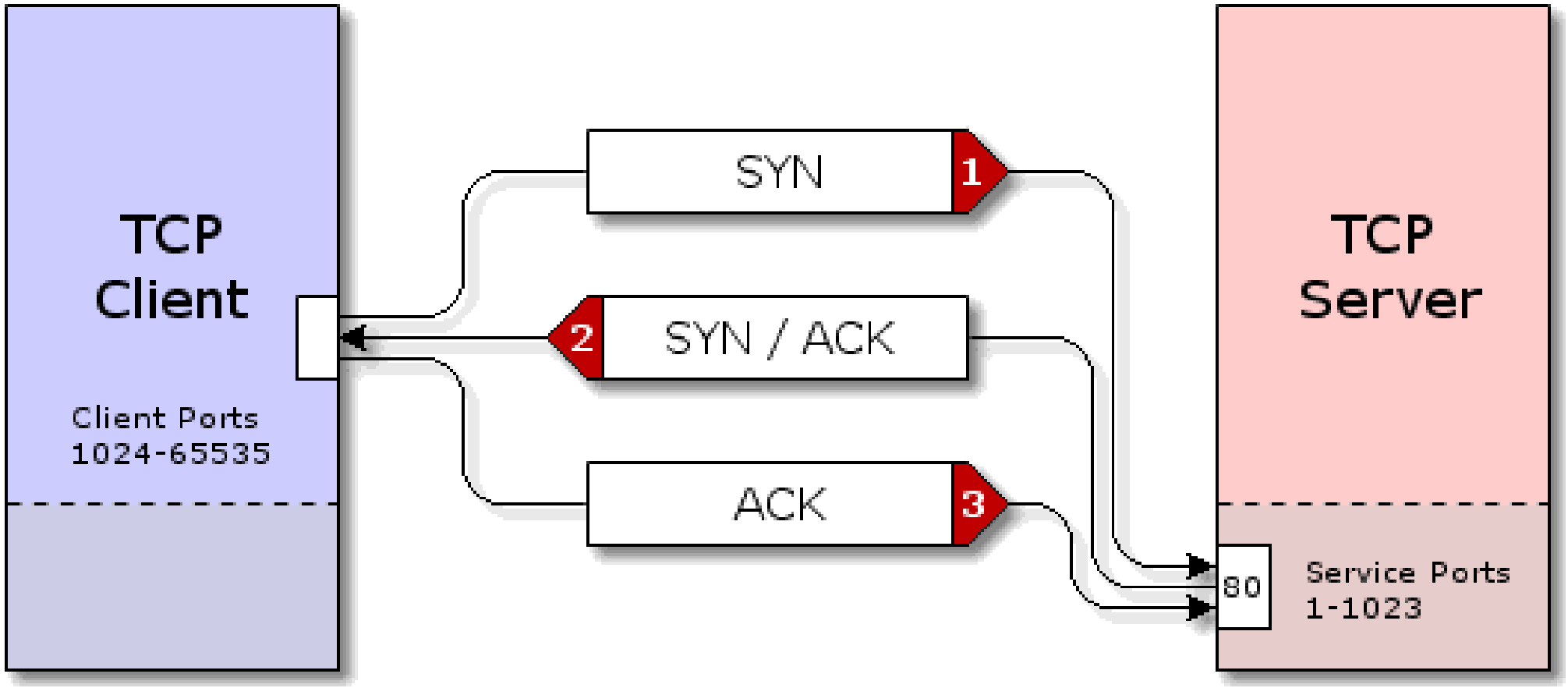
- Every entity must only access the resources need for its legitimate function and nothing more.
  - AKA, the most restrictive set of permissions

- An entity can be:
  - User
  - Program
  - Process
  - Local or Remote

Security auditing

- Auditing is testing your system to ensure that its behavior meets your security needs
- With local users, it can be easy to determine what privileges each user has, either by using commands or by viewing permissions (e.g., **ls –l**)
- For network security, it can be quite difficult since there are so many applications use the network

TCP Three-way Handshake



Source: https://tuxawy.files.wordpress.com/2012/04/tcp-connect1.gif

nmap

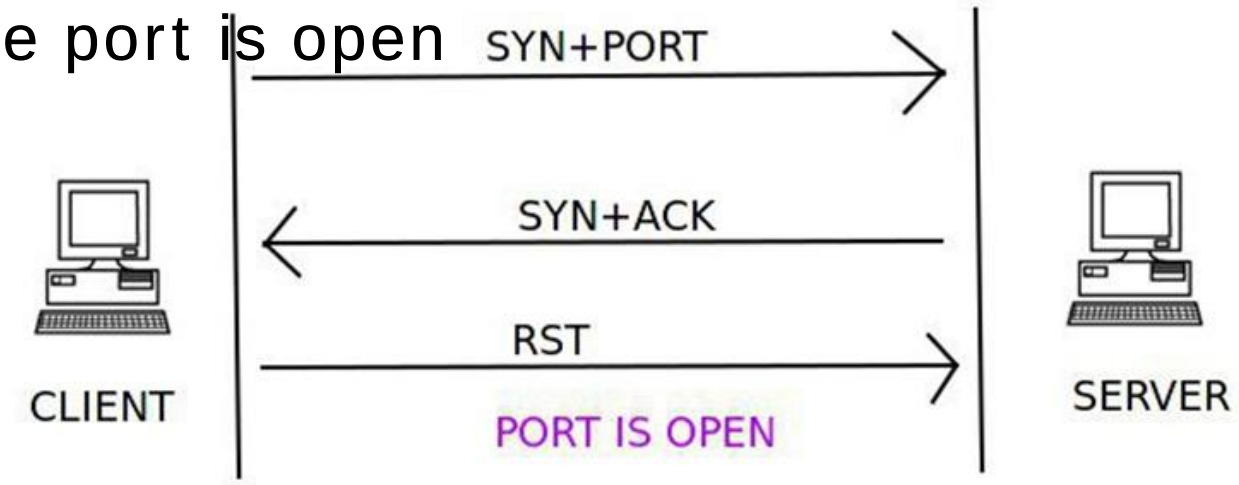
- “Network Mapper”
- Open-source tool for network discovery and security “auditing”
- Mainly used for port scanning

We can use nmap to see what ports are open

- **$ nmap –sS HOST**
  - TCP SYN scan
  - The most popular nmap function

- Half-opens connections to do the scan
  - Send a SYN to every port on HOST
  - If you get a SYN/ACK, the port is open

- Requires root



Running nmap –sS for real

```
zak@HOST:~$ sudo nmap -sS bone

Starting Nmap 6.40 ( http://nmap.org ) at 2016-11-01 15:07 EDT
Nmap scan report for bone (192.168.7.2)
Host is up (0.0079s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3000/tcp open  ppp
9090/tcp open  zeus-admin
MAC Address: C8:A0:30:B7:F9:71 (Texas Instruments)

Nmap done: 1 IP address (1 host up) scanned in 1.73 seconds
zak@HOST:~$
```

What if I forgot the IP address of my board?

- I could use nmap to find it
- Let's say I remember the beaglebone is on the 192.168.7.0/24 network
- I can scan it with **nmap –n –A –PS22 192.168.7.0/24**
  - -n: no DNS resolution
  - -A: use OS detection, version detection, script scanning and traceroute
  - -PS22: TCP SYN ping on Port 22

nmap –n –A –PS22 192.168.7.0/24

```
Nmap scan report for 192.168.7.2
Host is up (0.0092s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
80/tcp   open  http?
|_http-methods: No Allow or Public header in OPTIONS response (status code 404)
|_http-title: Introduction to BeagleBoard.org
3000/tcp open  ppp?
9090/tcp open  zeus-admin?
3 services unrecognized despite returning data. If you know the service/version,
 please submit the following fingerprints at http://www.insecure.org/cgi-bin/ser
vicefp-submit.cgi :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=6.40%I=7%D=11/1%Time=5818F453%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,F01,"HTTP/1\.1\x20200\x20OK\r\nX-Powered-By:\x20Express\r\nAccep
SF:t-Ranges:\x20bytes\r\nCache-Control:\x20public,\x20max-age=0\r\nLast-Mo
SF:dified:\x20Fri,\x2008\x20Jul\x202016\x2020:53:08\x20GMT\r\nETag:\x20W/\
SF:"de0-155cc490f20\"\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\nC
SF:ontent-Length:\x203552\r\nDate:\x20Tue,\x2001\x20Nov\x202016\x2020:00:2
SF:2\x20GMT\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20html>\n<html><head
SF:>\n\x20\x20\x20\x20<title>Introduction\x20to\x20BeagleBoard\.org</title
.
```

Okay, great I know what ports are open

- How do I close them off?!?!

- Linux comes with a built in firewall
  - Managed using the “iptables” command
  - iptables commands build a “chain” that is processed when a network packet arrives

- Excellent description:
  - https://www.globo.tech/learning-center/linux-native-firewall-introduction-to-iptables/

If want to close port 3000 from the outside

- Run two commands:
  - iptables -A INPUT -s 192.168.7.0/24 -p tcp -m tcp --dport 3000 -j ACCEPT
  - iptables -A INPUT -p tcp -m tcp --dport 3000 -j REJECT –reject-with icmp-port-unreachable
- If you want to see which iptables rules are active
  - iptables –L
- To flush the rules and restore default operation
  - iptables -F

What if I want to use those ports sometimes?

- We can either make our rules less restrictive to open up access to more networks
  - Add another “–j ACCEPT” rule before the “-j REJECT” rule

- Alternatively, if we have SSH open, we could do ssh port forwarding

SSH Port Forwarding

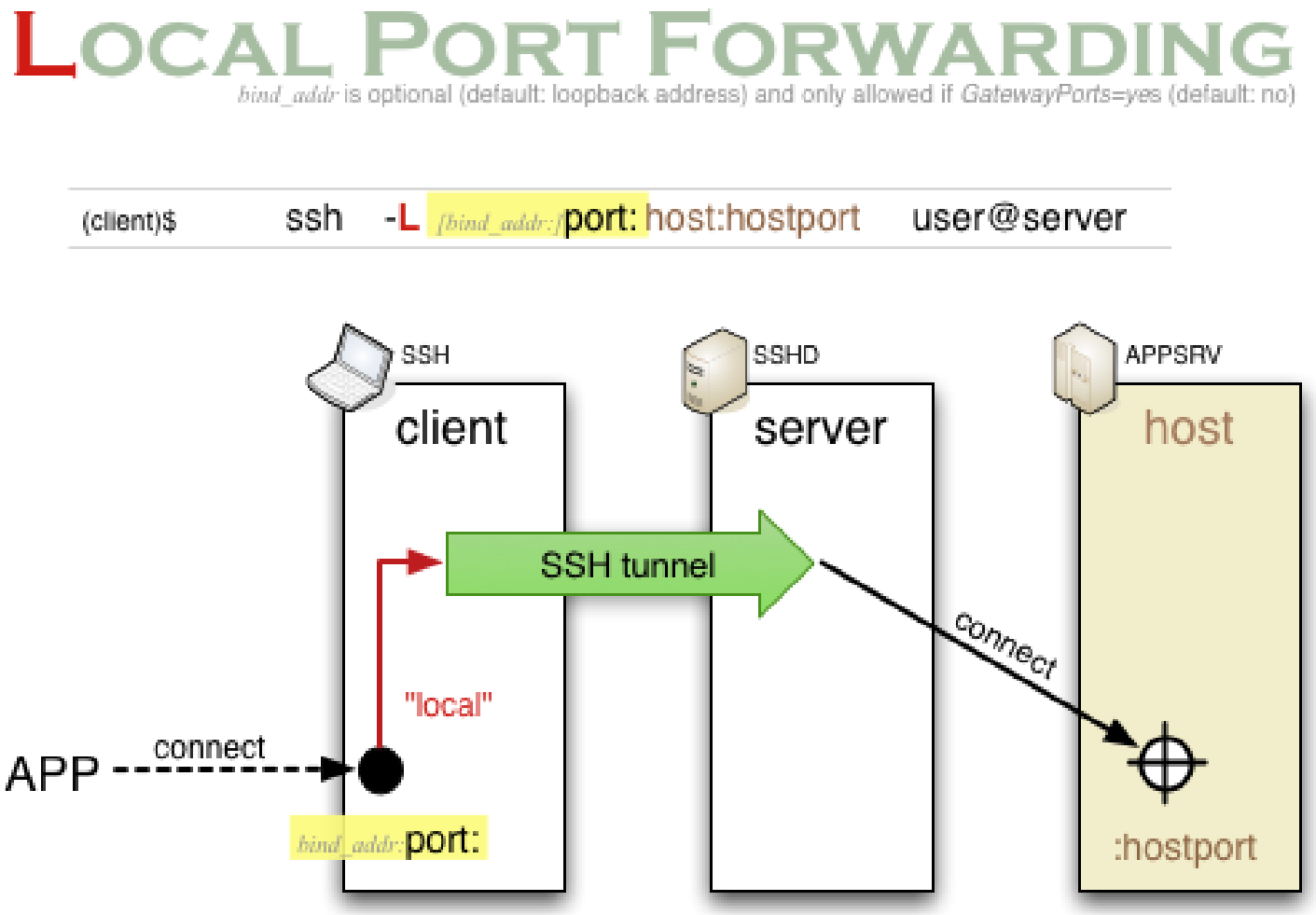


Image source: http://www.dirk-loss.de/ssh-port-forwarding.png

SSH Port Forwarding example

- So, to get to our port 3000, we would execute
  - **ssh bone –L3000:localhost:3000**

- This forwards port 3000 on the beaglebone …
  - We use “localhost” since the command takes the ssh server’s perspective
- and forwards it to port 3000 on the host
  - where you are sshing from

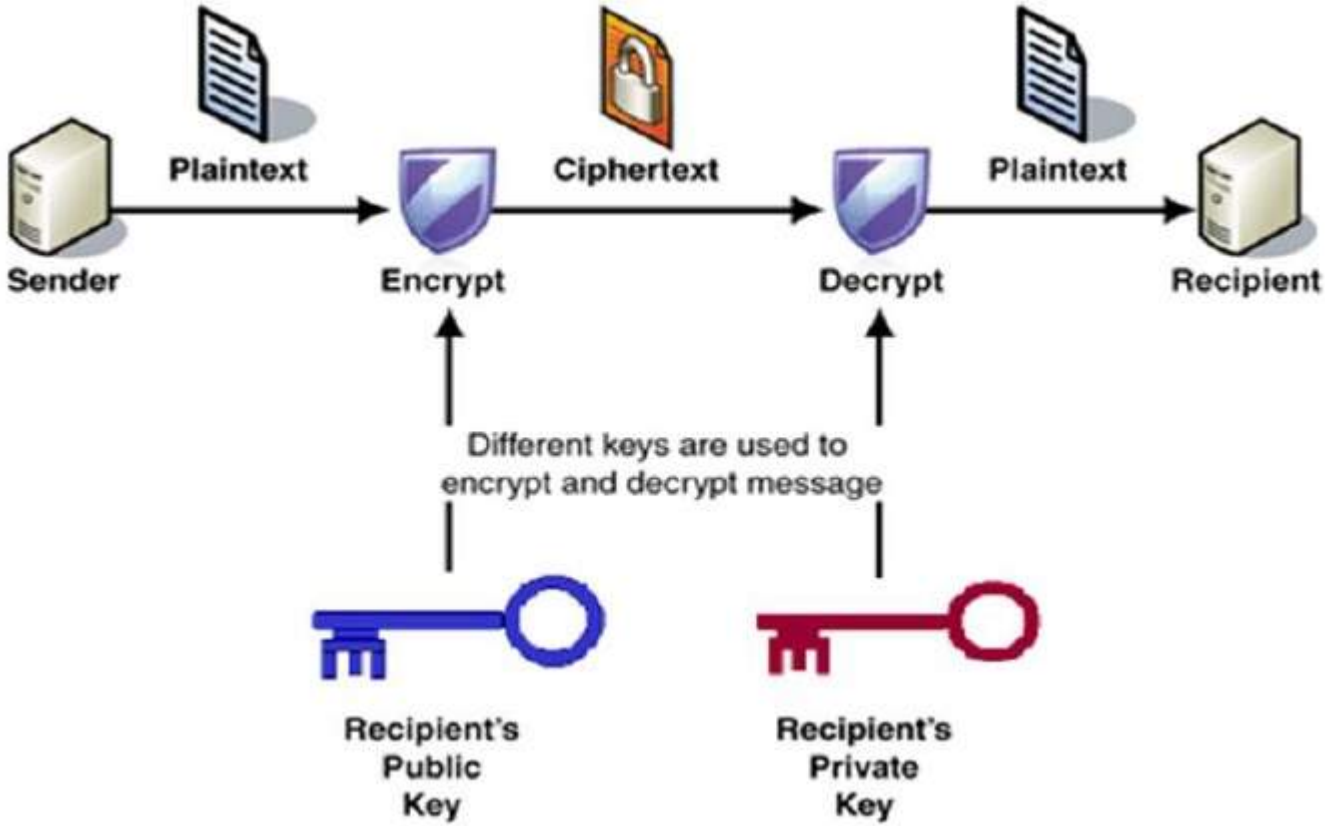
- This means we connect to port 3000 on the host to reach port 3000 on the bone, as long as we keep ssh open

Preventing brute-force attacks

- Fail2ban
  - Automatically sets up iptables rules
- Disable root ssh
  - /etc/ssh/sshd_config
  - Remember to restart ssh!
- Use a strong password
- Or... use public key authentication

SSH Public Key Authentication

- Built on public key cryptography
  - Keys are easy to generate and verify, but difficult to guess



Source: https://www.tutorialspoint.com/cryptography/public_key_encryption.htm

Using SSH Public Key Authentication

- Generating a key:
  - **ssh-keygen**
  - Can add a passphrase (recommended, look into ssh-agent if you do this)
- Using a key:
  - **ssh-copy-id SERVER**
    - Use your password once
    - Look at ~/.ssh/authorized_keys
- Very often, you'll see servers that don't ever use passwords
  - Cloud instances, etc…

Summary

- Embedded device security
- Principle of least privilege
- TCP handshake
- Port scanning
  - Nmap
- Firewall
  - Iptables
- Port forwarding
  - Using ssh
- Public Key Authentication

Random stuff: let's say I forgot my password

- The linux kernel has arguments just like any other program
- Grub bootloader lets you change the kernel's command line arguments