Bluetooth Security

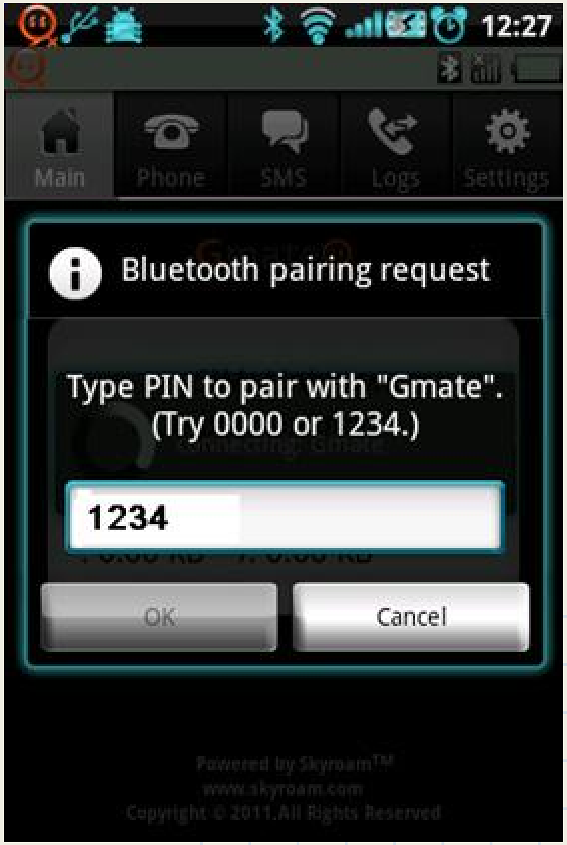
6.858 Final Project, Fall 2012

echai bendorff cathywu @ mit

Bluetooth security model

1. **Authorization**: user verification (PIN)
2. **Authentication**: PIN → link key
3. **Confidentiality**: link key → encryption

+



Bluetooth pairing request

Type PIN to pair with "Gmate".
(Try 0000 or 1234.)

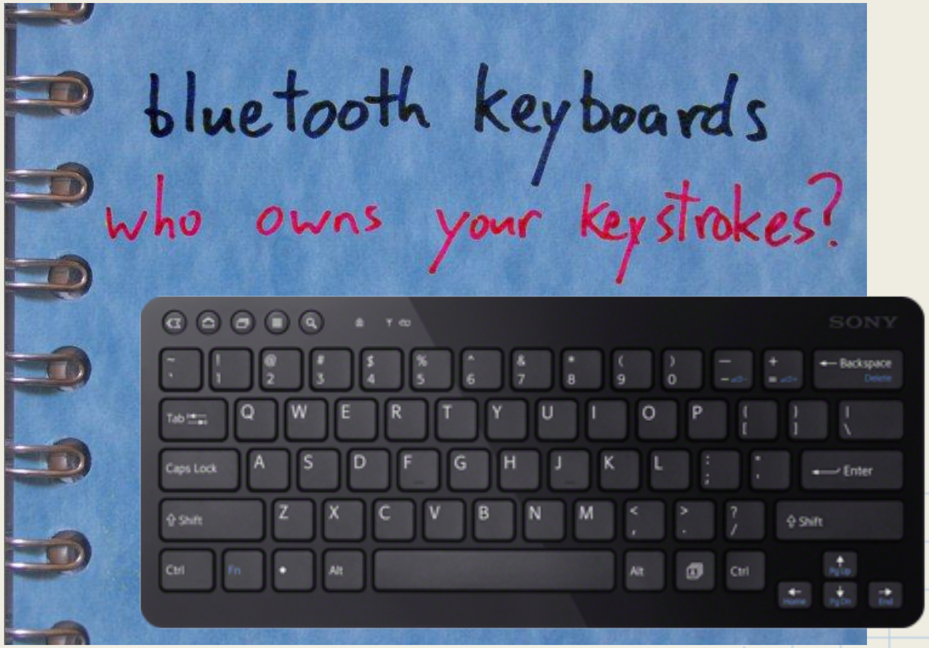
1234

Powered by Skyroam™
www.skyroam.com
Copyright © 2011.All Rights Reserved

Source NIST: Guide to Bluetooth Security

Bluetooth — secure?

- **What makes hacking Bluetooth hard?**
  - Channel hopping
  - Adaptive Frequency Hopping
  - Whitening
  - **Encryption**
  - Lack of affordable tools

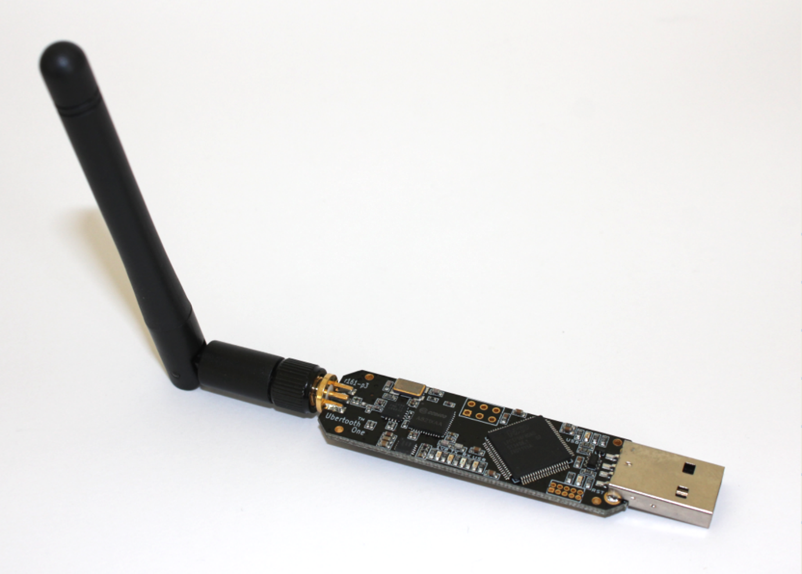


"*Vulnerabilities will be ignored until tools are available*" -- Wright's Law

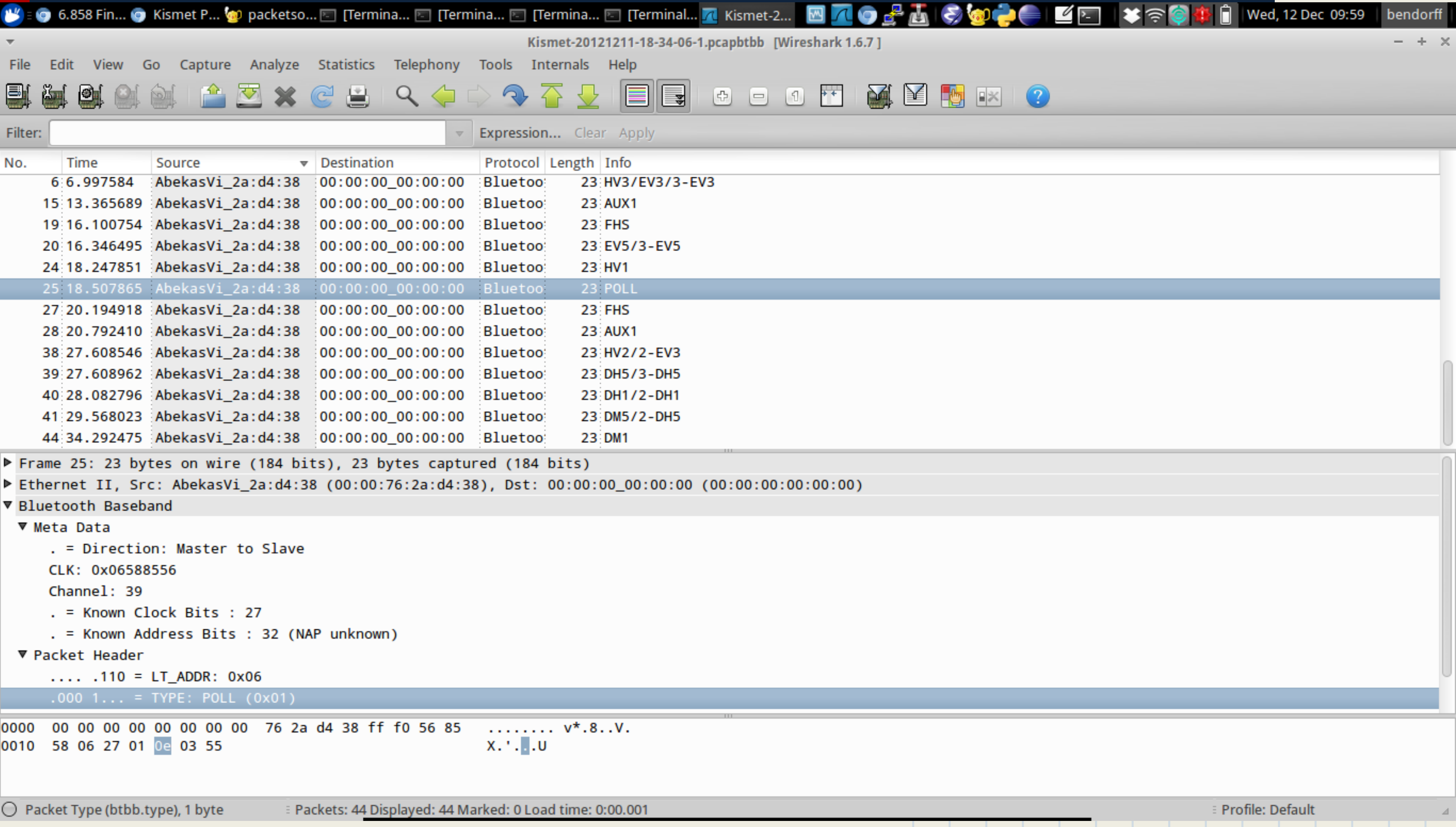
Source ShmooCon 2011: Project Ubertooth

Ubertooth + Kismet

- **Ubertooth: Bluetooth development platform** ($120, 2011)
- **Kismet: passive wireless sniffer**
- **Open source**
- **Kismet + Ubertooth**: no channel hopping in Kismet
  - Losing packets on other channels
- **Our implementatio**n: add channel hopping to Kismet + Ubertooth
  - Kismet can now follow a device
  - More packets can be captured and decoded



Sample Packet Capture



No.	Time	Source	Destination	Protocol	Length	Info
6	6.997584	AbekasVi_2a:d4:38	00:00:00_00:00:00	Bluetoo	23	HV3/EV3/3-EV3
15	13.365689	AbekasVi_2a:d4:38	00:00:00_00:00:00	Bluetoo	23	AUX1
19	16.100754	AbekasVi_2a:d4:38	00:00:00_00:00:00	Bluetoo	23	FHS
20	16.346495	AbekasVi_2a:d4:38	00:00:00_00:00:00	Bluetoo	23	EV5/3-EV5
24	18.247851	AbekasVi_2a:d4:38	00:00:00_00:00:00	Bluetoo	23	HV1
25	18.507865	AbekasVi_2a:d4:38	00:00:00_00:00:00	Bluetoo	23	POLL
27	20.194918	AbekasVi_2a:d4:38	00:00:00_00:00:00	Bluetoo	23	FHS
28	20.792410	AbekasVi_2a:d4:38	00:00:00_00:00:00	Bluetoo	23	AUX1
38	27.608546	AbekasVi_2a:d4:38	00:00:00_00:00:00	Bluetoo	23	HV2/2-EV3
39	27.608962	AbekasVi_2a:d4:38	00:00:00_00:00:00	Bluetoo	23	DH5/3-DH5
40	28.082796	AbekasVi_2a:d4:38	00:00:00_00:00:00	Bluetoo	23	DH1/2-DH1
41	29.568023	AbekasVi_2a:d4:38	00:00:00_00:00:00	Bluetoo	23	DM5/2-DH5
44	34.292475	AbekasVi_2a:d4:38	00:00:00_00:00:00	Bluetoo	23	DM1

```
▶ Frame 25: 23 bytes on wire (184 bits), 23 bytes captured (184 bits)
▶ Ethernet II, Src: AbekasVi_2a:d4:38 (00:00:76:2a:d4:38), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▼ Bluetooth Baseband
  ▼ Meta Data
      . = Direction: Master to Slave
      CLK: 0x06588556
      Channel: 39
      . = Known Clock Bits : 27
      . = Known Address Bits : 32 (NAP unknown)
  ▼ Packet Header
      .... .110 = LT_ADDR: 0x06
      .000 1... = TYPE: POLL (0x01)
```

```
0000  00 00 00 00 00 00 00 00  76 2a d4 38 ff f0 56 85   ........ v*.8..V.
0010  58 06 27 01 0e 03 55                               X.'...U
```

Packet Type (btbb.type), 1 byte   Packets: 44 Displayed: 44 Marked: 0 Load time: 0:00.001   Profile: Default

Conclusions

- **Security implications of Project Ubertooth**
  - Passive Sniffing
  - Packet Injection
- **Bluetooth: Safe for now?**
  - Project Ubertooth still under active development
    - Packet Injection tool still premature
    - Encryption
- **Why is hacking Bluetooth important?**

Conclusions

- **Security implications of Project Ubertooth**
  - Passive Sniffing
  - Packet Injection
- **Bluetooth: Safe for now?**
  - Project Ubertooth still under active development
    - Packet Injection tool still premature
    - Encryption
- **Why is hacking Bluetooth important?**

Many many thanks!

- Professor Zeldovich
- Michael Ossmann (Ubertooth)
- Dominic Spill (Ubertooth)
- Mike Kershaw (Kismet)