

PACKETCRAFT[®]
WORLD-LEADING WIRELESS

Analysis of Bluetooth Channel Sounding

A New Bluetooth Feature for High Accuracy Distance Measurement

John Yi | CEO | Packetcraft

Agenda

- Intro
- Use Cases
- Concepts
- Link Layer
- Analysis
- Summary


Intro

John Yi architected and implemented the Bluetooth LE Link Layer since v4.0 and participates in the Bluetooth Core Working Group for about 15 years.

A horizontal timeline with an arrow pointing right, marked with three points: 2009, 2015, and 2019. Above the timeline are the logos for wicentric (with a snowflake icon), arm, and PACKETCRAFT® (with a cube icon).

Over a Decade of Industry Leadership

Name	Role	Experience
 John Yi	CEO & Founder	25+ Years
 Jason Hillyard	VP Business Development & Cofounder	25+ Years
 Bob Brand	VP Software Engineering	30+ Years
 Dlight Ting	Principal Software Engineer	25+ Years


PACKETCRAFT®

Packetcraft is a software company developing and licensing protocol stacks and solution software for Bluetooth and other wireless technologies.

Use Cases

- Applications

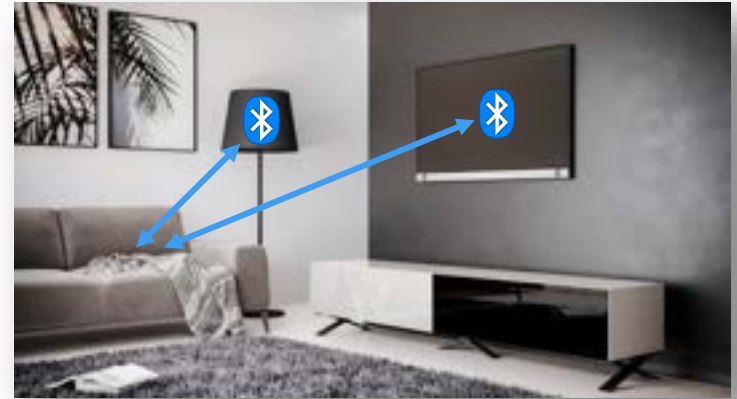
- Secure Access, e.g., car, building
- Real-Time Location System (RTLS), e.g., asset management, warehouse
- Indoor Positioning System (IPS)

- Device Requirements

- Single antenna, but works better with more paths
- Low complexity reflector (initiator runs algorithm)
- Operates at typical walking speed



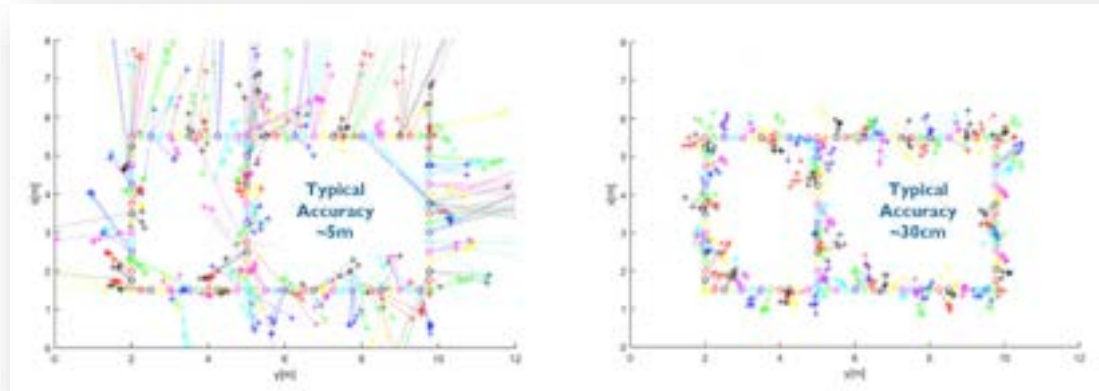
“Hey Siri, Where are my keys?”



“It’s in the living room,”
“7 feet from the TV.”

Use Cases – Accuracy

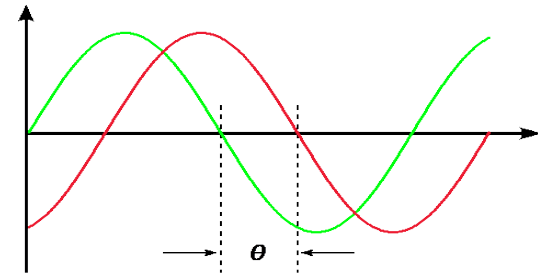
- Proximity Detection
- Accuracy ~30-cm



Credit: Imec

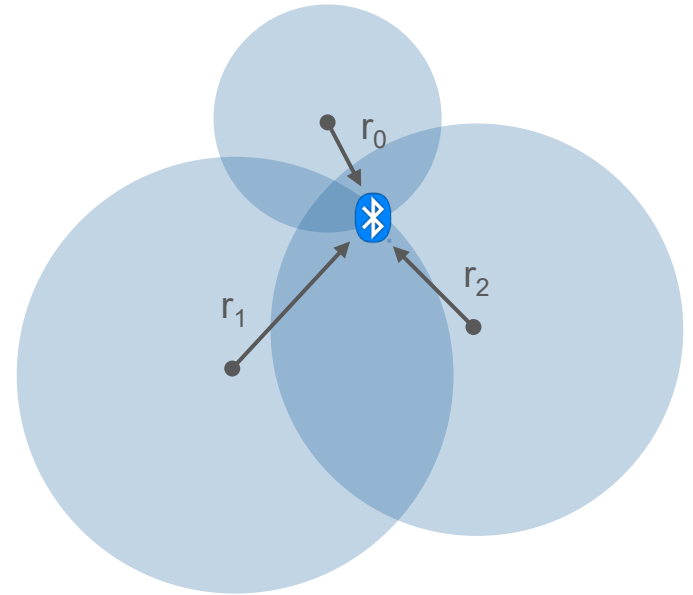
Concepts – Multipath

- RF impairment due to signal reflections, diffractions, and scattering
- Arrival at the receiver appears to have a longer path
- Dependent on frequency



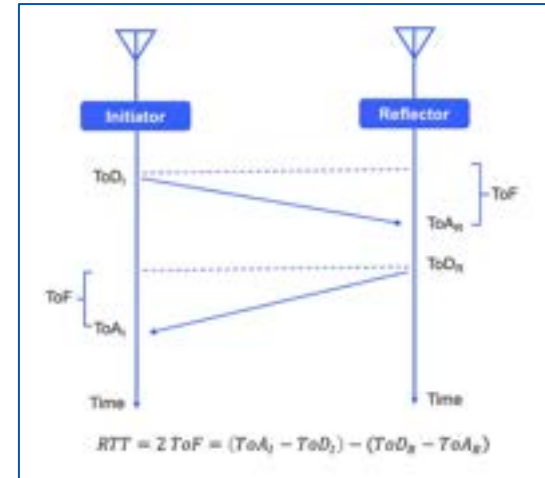
Concepts – Trilateration

- A moving device calculates its position using distance (r_x) from three fixed location devices
- Example: mobile devices can find indoor position using Bluetooth Beacons today with an accuracy of 4 meters under certain environmental conditions



Concepts – Round Trip Time (RTT)

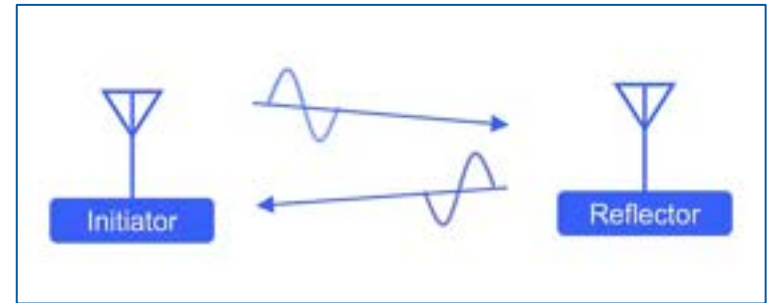
- Time of Flight (ToF)



Credit: Silicon Labs

Concepts – Phase-Based Ranging (PBR)

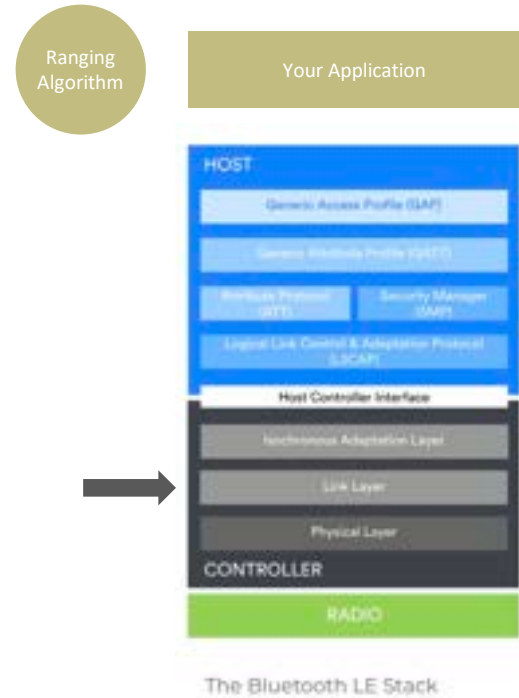
- Phase differences
- Amplitude
- More accurate than RTT



Credit: Silicon Labs

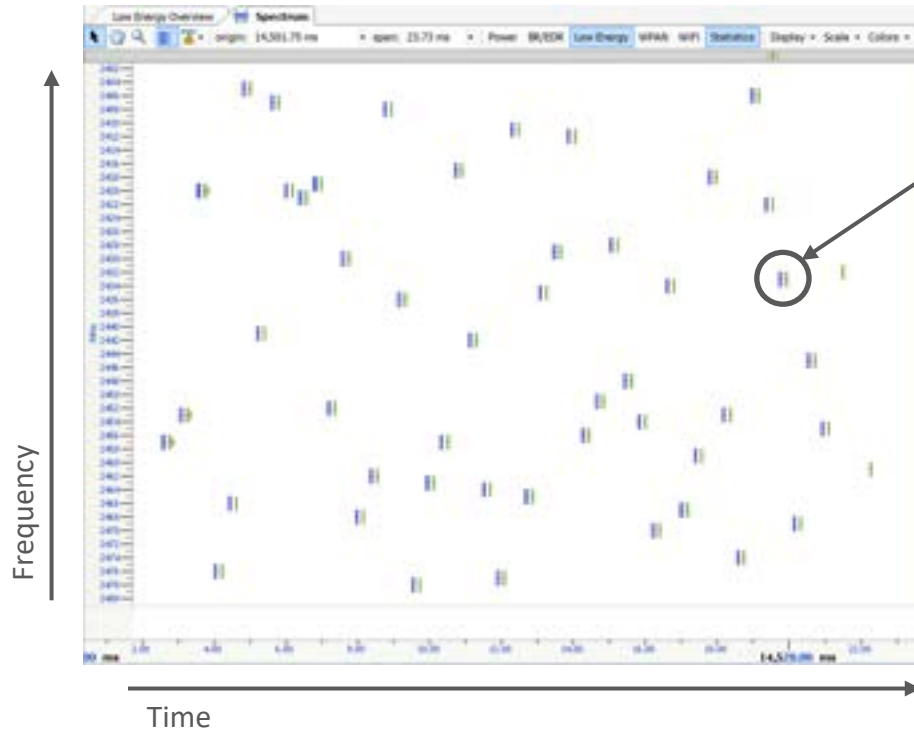
Link Layer – Context

- Transports
 - Connectionless (Broadcast): ADV, PA, PAWR, BIS
 - Connection Oriented (Peer-to-Peer): ACL, CIS, CS
- Medium Access
- State Machines



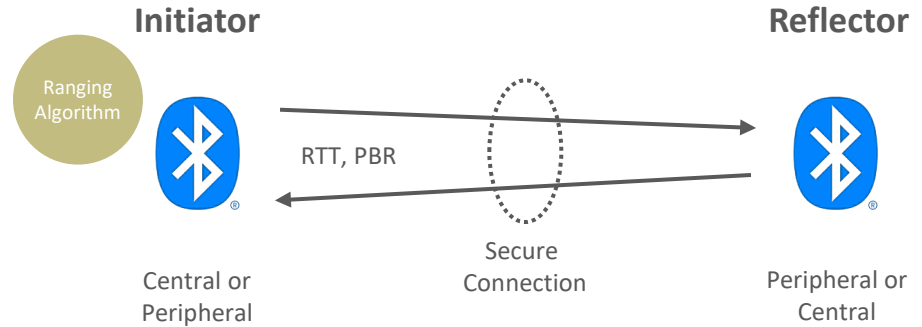
Link Layer – Communication Fundamentals

- Time
- Space – Frequency
- Coding – Access Address
- Modulation – PHY



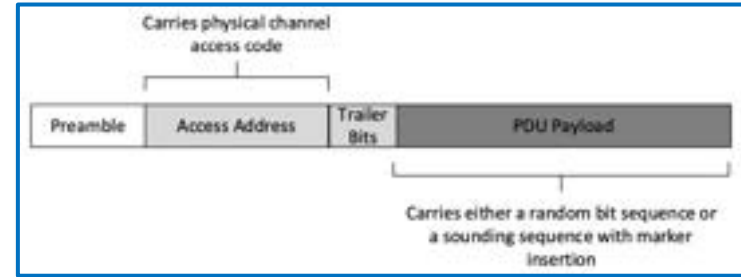
Link Layer – Roles and Modes

- Mode 0 - Calibrate
- Mode 1 – RTT
- Mode 2 – PBR
- Mode 3 – RTT + PBR (optional)



Link Layer – Packet Structure

- Compared to ADV and ACL
 - Preamble – no change
 - Access Address – cryptographically generated
 - Trailer – 4 bits
 - Payload – nibble multiple
 - CRC – not present
 - Whitening is disabled



A CS SYNC followed by a CS tone is shown in Figure 2.7. The CS SYNC has two mode-specific variations: a CS_SYNC_0_R, as described in Section 4.3.1 [Channel Sounding step mode-2], and a CS_SYNC_3_I, as described in Section 4.3.4 [Channel Sounding step mode-3].



Figure 2.7: CS SYNC followed by a CS tone

A CS tone followed by a CS SYNC is shown in Figure 2.8. In this case, the CS SYNC occurrence is the CS_SYNC_3_R as described in Section 4.3.4 [Channel Sounding step mode-3].

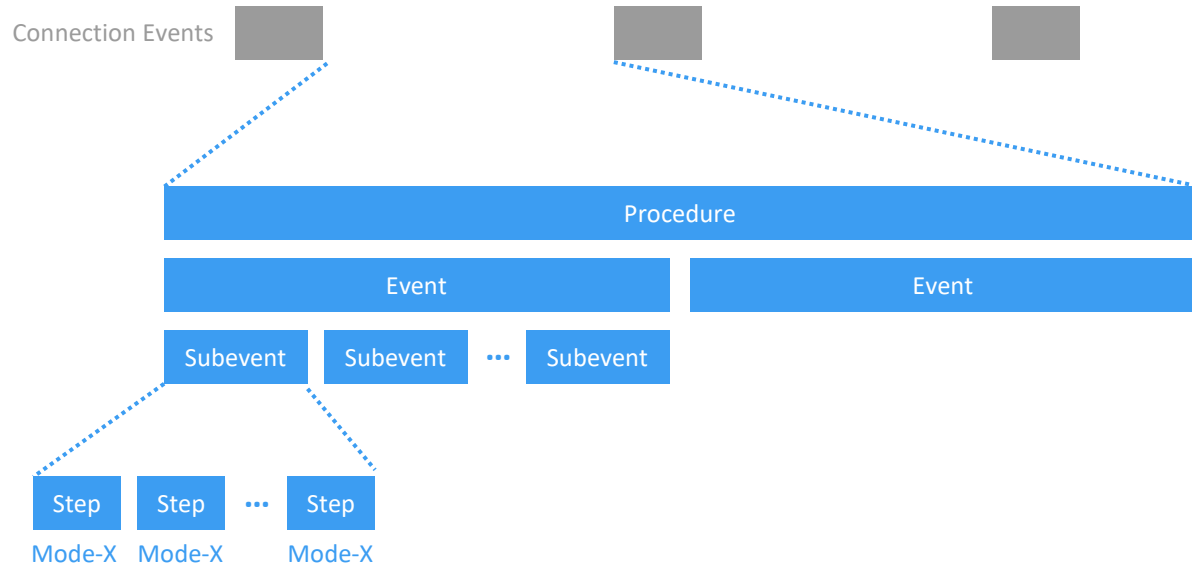


Figure 2.8: CS tone followed by a CS SYNC

Source: Bluetooth Channel Sounding CR_PR, 2023-06-22

Link Layer – Packet Organization

- Procedure
- Event
- Subevent
- Steps



Analysis

- Secure Connection prerequisite required
- Channel Sounding Procedure
 - Exchange Capabilities
 - Exchange Security
 - Negotiate Configuration
 - Exchange Measurements (repeats)

Item
LE-C Transfer (Encryption Request, Rnd=0xABCDEF1234567890, EDIV=0x2474, SKDm=0x2C9653)
LE-C Transfer (Encryption Response, SKDi=0x06B6EDCD223C4C6E, IVs=0x7190BF34)
LE-C Transfer (Start Encryption Request)
LE-C Transfer (Start Encryption Response)
LE-C Transfer (Start Encryption Response)
LE-C Transfer (CS Capabilities Request, Antennas=1 x 1, Initiator, Reflector, T_SW=10 us)
LE-C Transfer (CS Capabilities Response, AA Only=4 / 10 ns, Sounding=4 / 10 ns, Random=4 / 10 ns)
LE-C Transfer (CS Security Request, Central, IV=0x3E7F5186E0CA0B3B, IN=0x8673840D, PV=0x...)
LE-C Transfer (CS Security Response, Peripheral, IV=0x339AB3156DE2103C, IN=0xDCD9F145, PV=...)
LE-C Transfer (CS Config Request, Config=2, Main=1, PHY=LE 1M, AA only timing, #3b, TP1=145)
LE-C Transfer (CS Config Response, Config=2)
LE-C Transfer (CS Request, Config=2, Event=97, Ofs Min=1.54 ms, Ofs Max=1.54 ms, Duration=...)
LE-C Transfer (CS Response, Config=2, Event=97, Ofs Min=1.54 ms, Ofs Max=1.54 ms, Int=9, Su...)
LE-C Transfer (CS Indication, Config=2, Event=97, Ofs=1.54 ms, Subs=1, Len=20 ms, Act=0, LE ...)

Analysis

- Anti Spoofing
 - Pseudorandom Channel (CSA #3)
 - Pseudorandom AA generation
 - Subevent sub-mode insertion
 - Tone Extension Slot present
 - Antenna path permutation index
 - Pseudorandom Sounding Sequence markers
 - Random Bit Sequence
- Normalized Attack Detector Metric (NADM)

The screenshot displays a network analysis tool interface with a table of Bluetooth packets. The table has columns for 'Item', 'Access Address', 'RF Chan', and 'Time'. The 'Access Address' and 'RF Chan' columns are highlighted with red boxes. Below the table, a Bluetooth packet capture is shown with a red box around a specific packet.

Item	Access Address	RF Chan	Time
Channel Sounding Procedure (P=55, Mode=0, Step=0, Subevent=0, Event=0)			14.3
CS_SYNC (0x00004100, Coarse, Ch=55, Mode=0, Step=0, Subevent=0, Event=0)	0x00004100	55	14.3
CS_SYNC (0x00004100, Coarse, Ch=55, Mode=0, Step=0, Subevent=0, Event=0)	0x00004100	55	14.3
CS_SYNC (0x00004100, Coarse, Ch=55, Mode=0, Step=0, Subevent=0, Event=0)	0x00004100	55	14.3
Time (Duration=84 us, Ch=55, Mode=0, Step=0, Subevent=0, Event=0)			14.3
Channel Sounding Step (P=51, Mode=0, Step=1, Subevent=0, Event=0)			14.3
CS_SYNC (0x00004100, Coarse, Ch=51, Mode=0, Step=1, Subevent=0, Event=0)	0x00004100	51	14.3
CS_SYNC (0x00004100, Coarse, Ch=51, Mode=0, Step=1, Subevent=0, Event=0)	0x00004100	51	14.3
Time (Duration=83 us, Ch=51, Mode=0, Step=1, Subevent=0, Event=0)			14.3
Channel Sounding Step (P=18, Mode=0, Step=2, Subevent=0, Event=0)			14.3
CS_SYNC (0x00004100, Coarse, Ch=18, Mode=0, Step=2, Subevent=0, Event=0)	0x00004100	18	14.3
CS_SYNC (0x00004100, Coarse, Ch=18, Mode=0, Step=2, Subevent=0, Event=0)	0x00004100	18	14.3
Time (Duration=83 us, Ch=18, Mode=0, Step=2, Subevent=0, Event=0)			14.3
Channel Sounding Step (P=74, Mode=0, Step=3, Subevent=0, Event=0)			14.3
CS_SYNC (0x00004100, Coarse, Ch=74, Mode=0, Step=3, Subevent=0, Event=0)	0x00004100	74	14.3
CS_SYNC (0x00004100, Coarse, Ch=74, Mode=0, Step=3, Subevent=0, Event=0)	0x00004100	74	14.3
Time (Duration=83 us, Ch=74, Mode=0, Step=3, Subevent=0, Event=0)			14.3
Channel Sounding Step (P=44, Mode=0, Step=4, Subevent=0, Event=0)			14.3
CS_SYNC (0x00004100, Coarse, Ch=44, Mode=0, Step=4, Subevent=0, Event=0)	0x00004100	44	14.3
CS_SYNC (0x00004100, Coarse, Ch=44, Mode=0, Step=4, Subevent=0, Event=0)	0x00004100	44	14.3
Time (Duration=83 us, Ch=44, Mode=0, Step=4, Subevent=0, Event=0)			14.3
Channel Sounding Step (P=3, Mode=0, Step=5, Subevent=0, Event=0)			14.3
CS_SYNC (0x00004100, Coarse, Ch=3, Mode=0, Step=5, Subevent=0, Event=0)	0x00004100	3	14.3
CS_SYNC (0x00004100, Coarse, Ch=3, Mode=0, Step=5, Subevent=0, Event=0)	0x00004100	3	14.3
Time (Duration=83 us, Ch=3, Mode=0, Step=5, Subevent=0, Event=0)			14.3
Channel Sounding Step (P=29, Mode=0, Step=6, Subevent=0, Event=0)			14.3
CS_SYNC (0x00004100, Coarse, Ch=29, Mode=0, Step=6, Subevent=0, Event=0)	0x00004100	29	14.3
CS_SYNC (0x00004100, Coarse, Ch=29, Mode=0, Step=6, Subevent=0, Event=0)	0x00004100	29	14.3
Time (Duration=83 us, Ch=29, Mode=0, Step=6, Subevent=0, Event=0)			14.3
Channel Sounding Step (P=5, Mode=0, Step=7, Subevent=0, Event=0)			14.3
CS_SYNC (0x00004100, Coarse, Ch=5, Mode=0, Step=7, Subevent=0, Event=0)	0x00004100	5	14.3
CS_SYNC (0x00004100, Coarse, Ch=5, Mode=0, Step=7, Subevent=0, Event=0)	0x00004100	5	14.3
Time (Duration=83 us, Ch=5, Mode=0, Step=7, Subevent=0, Event=0)			14.3

Summary

- High accuracy – about 30-cm with specialized algorithms
- Ubiquity of Bluetooth
 - Beacons can add fine ranging
 - Your phone is your Digital Key
- Highly secure with built in anti-spoofing
- Channel Sounding air trace available for download – *coming soon*
Sign up for Packetcraft's newsletter: www.packetcraft.com

References

- Channel Sounding CR_PR (Draft)
<https://www.bluetooth.com/specifications/specs/channel-sounding-cr-pr/>
- Bluetooth Core Specification 5.4 (Adopted)
<https://www.bluetooth.com/specifications/specs/core-specification-5-4/>
- Introducing: The Bluetooth Low Energy Primer
<https://www.bluetooth.com/blog/introducing-the-bluetooth-low-energy-primer/>
- Bluetooth Channel Sounding – A Step Towards 10-cm Ranging Accuracy for Secure Access, Digital Key, and Proximity Services
<https://www.bluetooth.com/blog/bluetooth-channel-sounding-a-step-towards-10-cm-ranging-accuracy-for-secure-access-digital-key-and-proximity-services/>
- Trilateration
<https://en.wikipedia.org/wiki/Trilateration>
- Multipath propagation
https://en.wikipedia.org/wiki/Multipath_propagation
- How Does Channel Sounding Work?
<https://www.silabs.com/wireless/bluetooth/channel-sounding>

Thank you!

Questions?

John Yi | Packetcraft
sales@packetcraft.com



The Bluetooth® word mark and logos are registered trademarks owned by the Bluetooth SIG, Inc. and any use of such marks by Ellisis is under license Other trademarks and trade names are those of their respective owners.