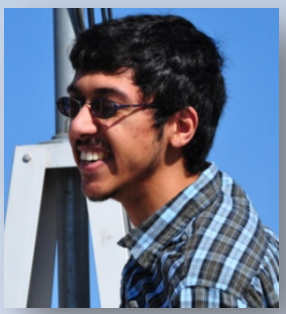
Secure PNT for Autonomous Systems

Todd Humphreys | Aerospace Engineering
The University of Texas at Austin

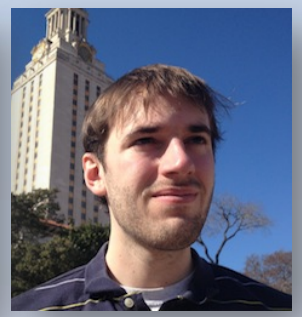
Stanford PNT Challenges and Opportunities Symposium | November 14, 2013

Acknowledgements

University of Texas Radionavigation Lab graduate students **Jahshan Bhatti, Kyle Wesson, Ken Pesyna, Zak Kassas, Daniel Shepard, and Andrew Kerns**





Master Andrew Schofield,

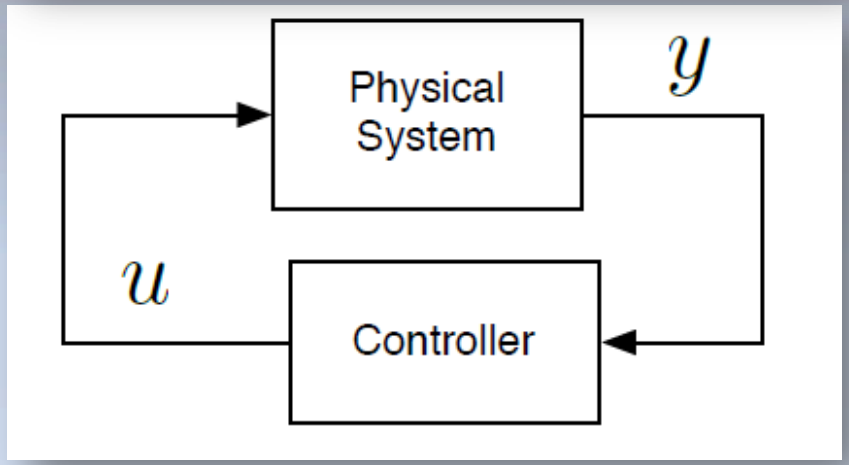
The White Rose of Drachs

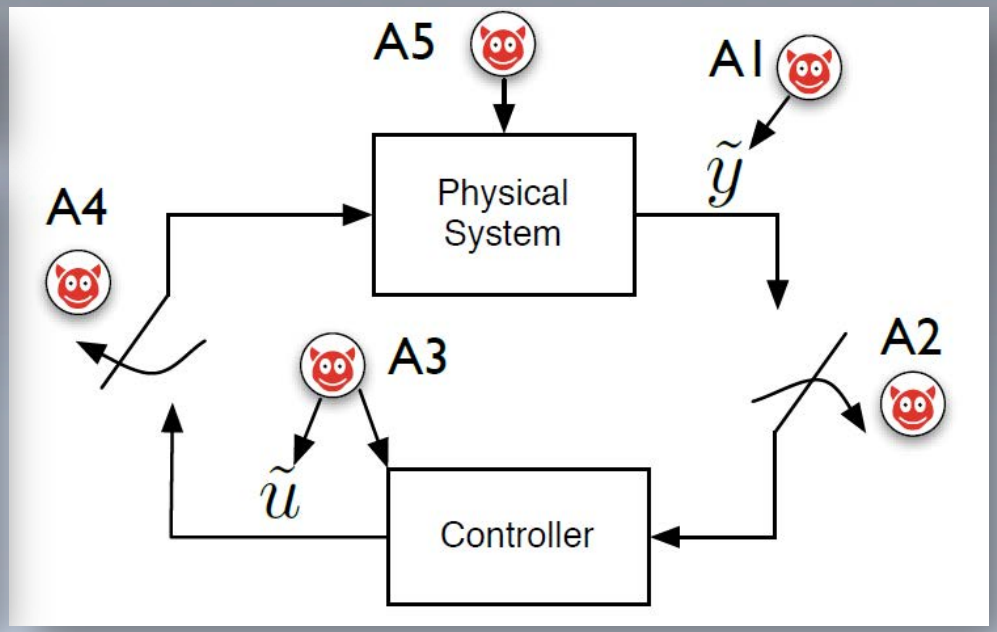
"routine UAS operations will not require the creation of a new special airspace, or modification of existing special use airspace"

Autonomous Control System Security

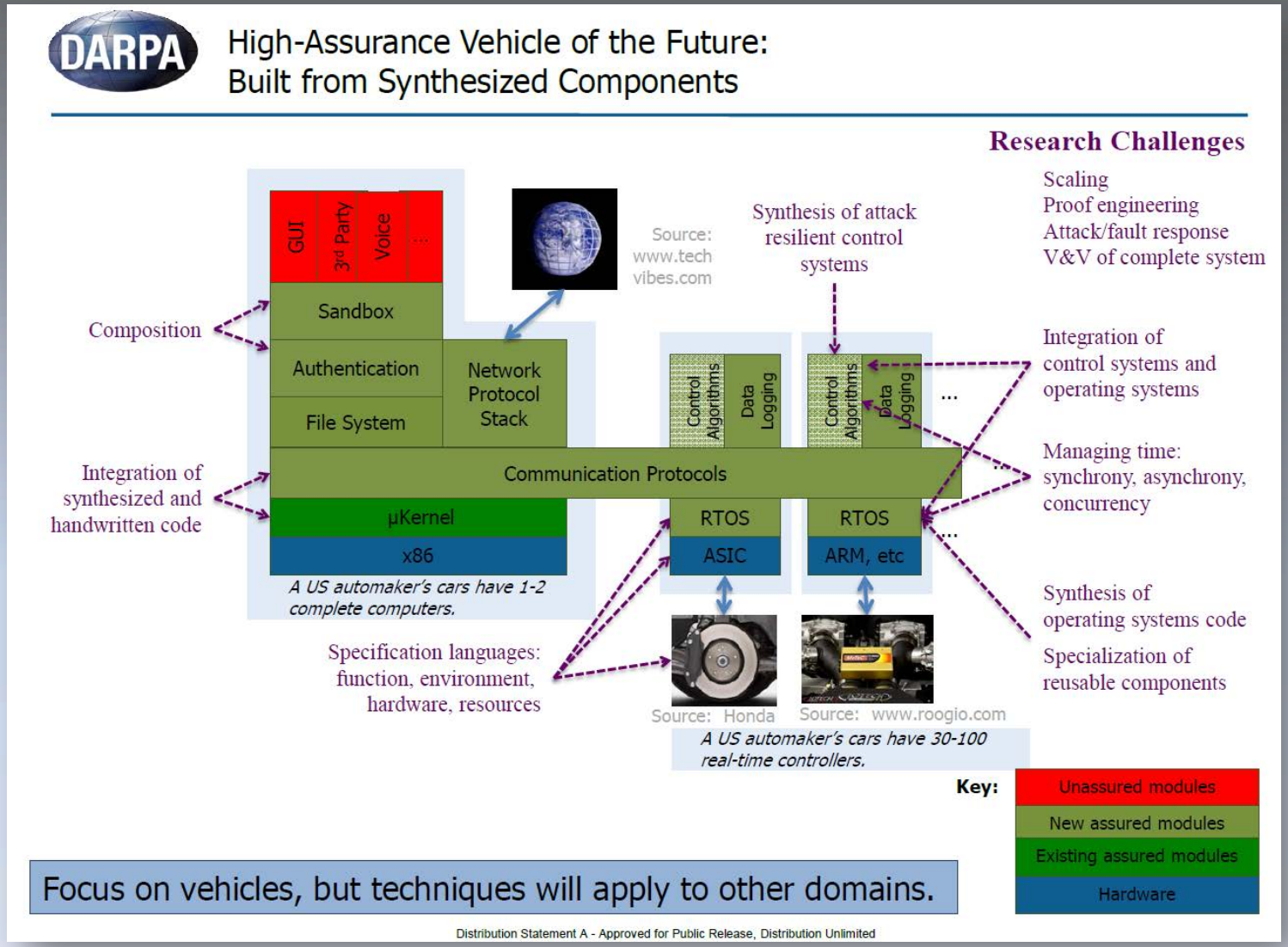
Secure Control: Towards Survivable Cyber-Physical Systems*

Alvaro A. Cárdenas Saurabh Amin Shankar Sastry
University of California, Berkeley





The general concept of secure control covers any manipulation of y and u (e.g, deception and DoS attacks), *but almost all research is focused on attacks on the communications and computer networks.*



DARPA's $60M HACMS program is focused on high-assurance code and network protocols, but what about the *sensors*?

Security research in the UT Radionavigation Laboratory is concerned with *field attacks:* attacks on the physical fields (e.g., electromagnetic, acoustic, pressure, etc.) measured by system sensors – especially *navigation system sensors*.

Example: Deep water drilling

- Dynamic positioning is a key technology for drilling and production
- In deepest waters, only GNSS and acoustic navigation sensors are practical
- The usual 3-system redundancy is waived so long as there are multiple DGPS receivers

Deepwater Horizon (~2009)

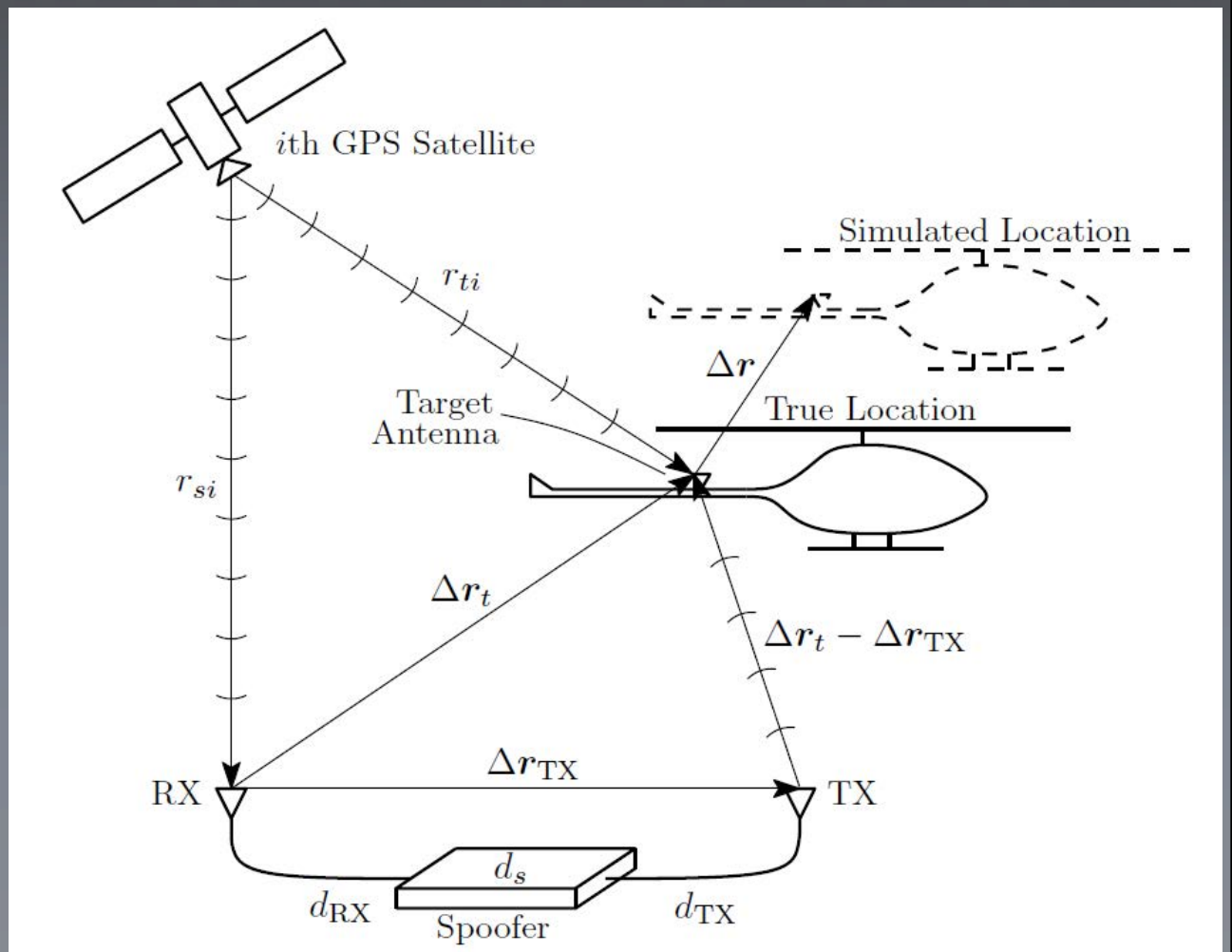
Vulnerable to a coordinated attack against GNSS and acoustic sensors

Deception and DoS field attacks have a long history in navigation warfare, but military defenses are of little use to the civilian community:

- Details of military protection schemes are classified
- Military defenses typically assume a trusted and trained user base willing to submit to onerous security protocols
- Fundamentally new technologies enable field attacks with which military has little experience (e.g., software-defined radio)

The civilian community will need to develop novel solutions to its own unique threats

UAV GPS Spoofing Attack



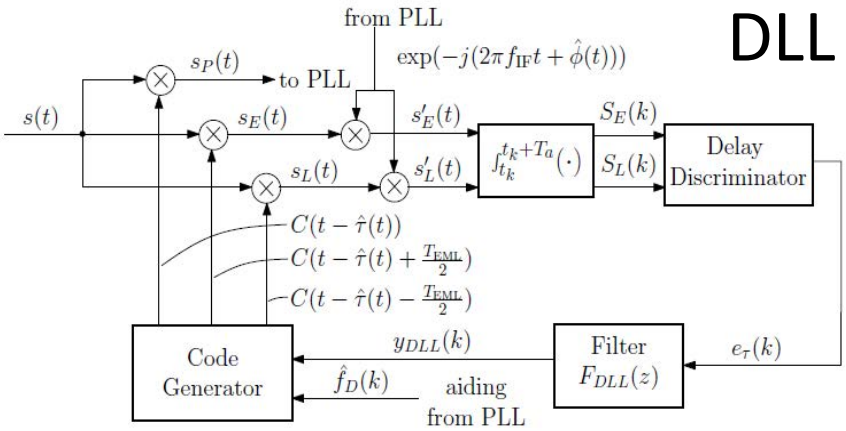
$$cd_i = r_{si} - r_{ti} + c(d_{\mathrm{RX}} + d_{\mathrm{TX}} + d_s) + ||\Delta \boldsymbol{r}_t - \Delta \boldsymbol{r}_{\mathrm{TX}}||$$

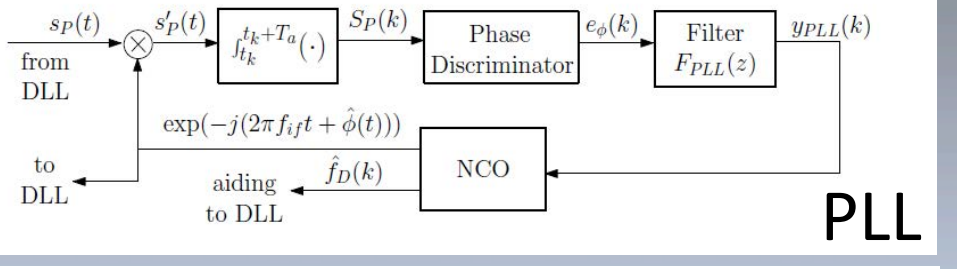

RADIONAVIGATION LABORATORY


BIG 12 CHAMPIONS '96 '05 '09
DARRELL K ROYAL - TEXAS MEMORIAL STADIUM
NATIONAL CHAMPIONS '63 '69 '70 '05
TEXAS
TEXAS

D.P. Shepard, J.A. Bhatti, T.E. Humphreys, A.A. Fansler, "Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks," Proc. ION GNSS, Nashville, TN, 2012.

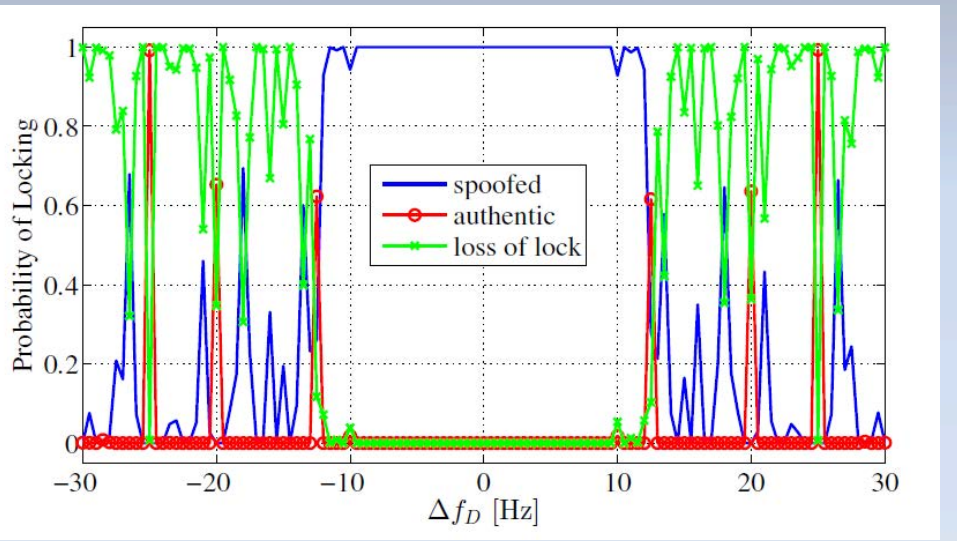
Covert GNSS Receiver Capture





η (dB)	Maximum velocity error (m/s)		
	Javad Delta	Trimble Juno SB	ublox Lea-6N
1	10	10	10
2	10	10	15
3	15	10	15

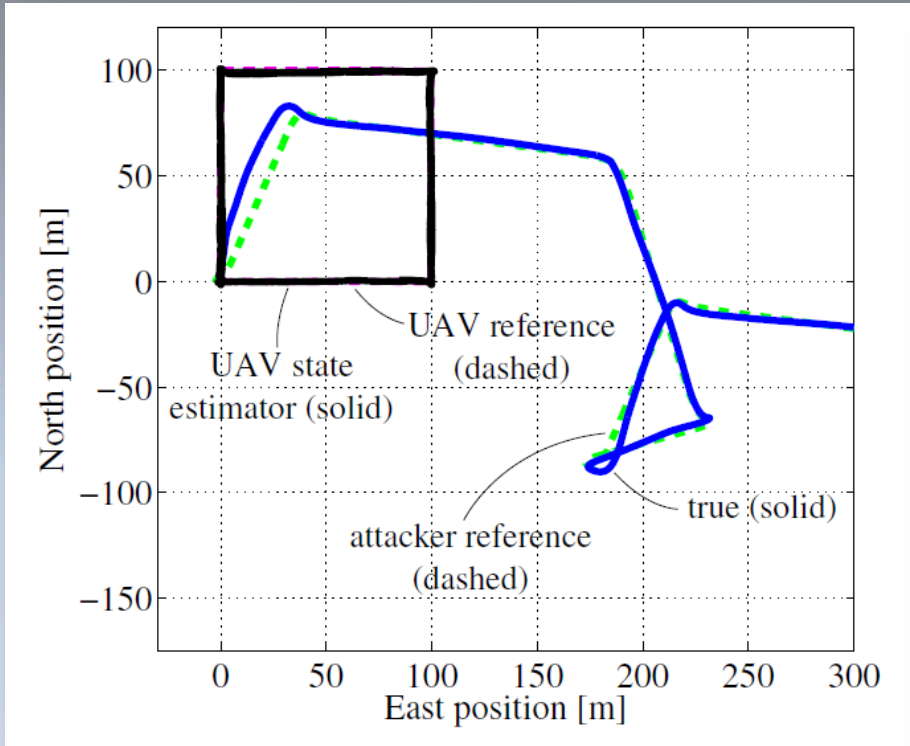
Results from live tests

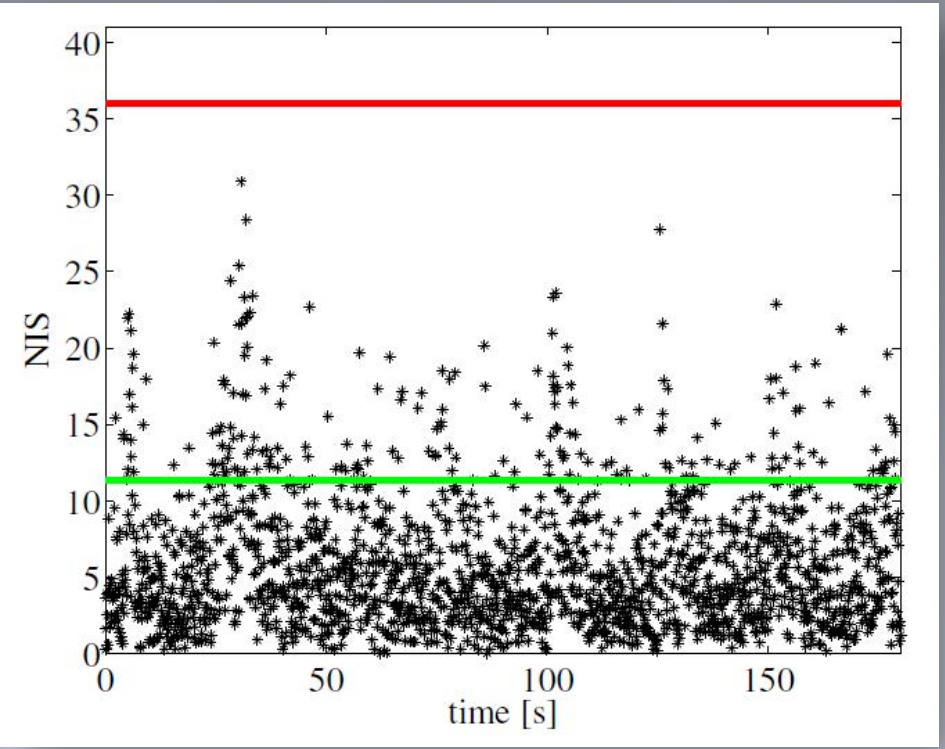


Allowable Doppler uncertainty

Ironically, commercial receivers' robustness makes them easier to covertly capture

Covert Post-Capture UAV Control





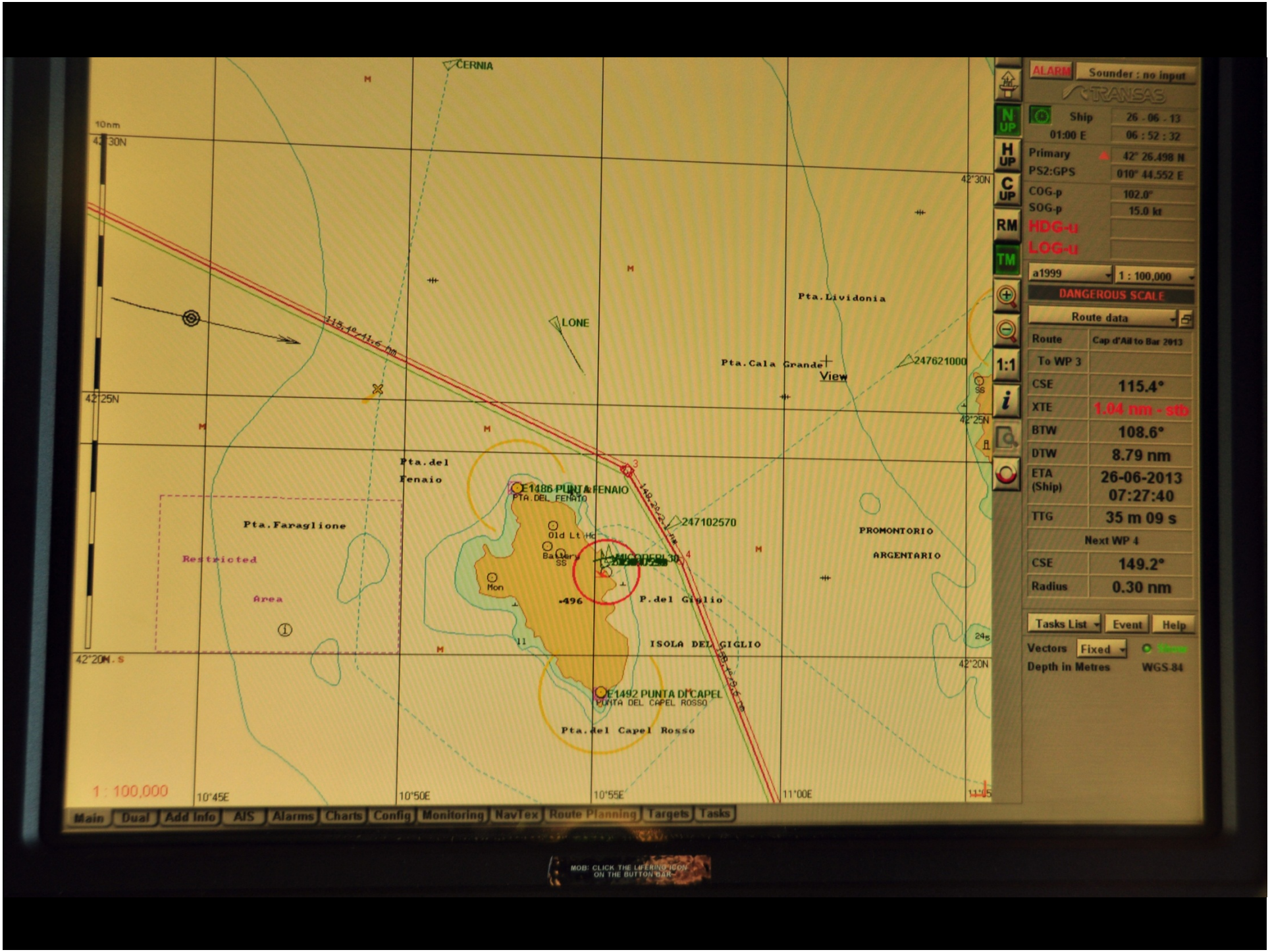
Stable covert post-captue UAV control is possible provided the spoofer can learn the target's flight pattern

Crashing is easier than control

A.J. Kerns, D.P. Shepard, J.A. Bhatti, T.E. Humphreys,
"Unmanned Aircraft Capture and Control via GPS Spoofing," Journal of Field Robotics, submitted.

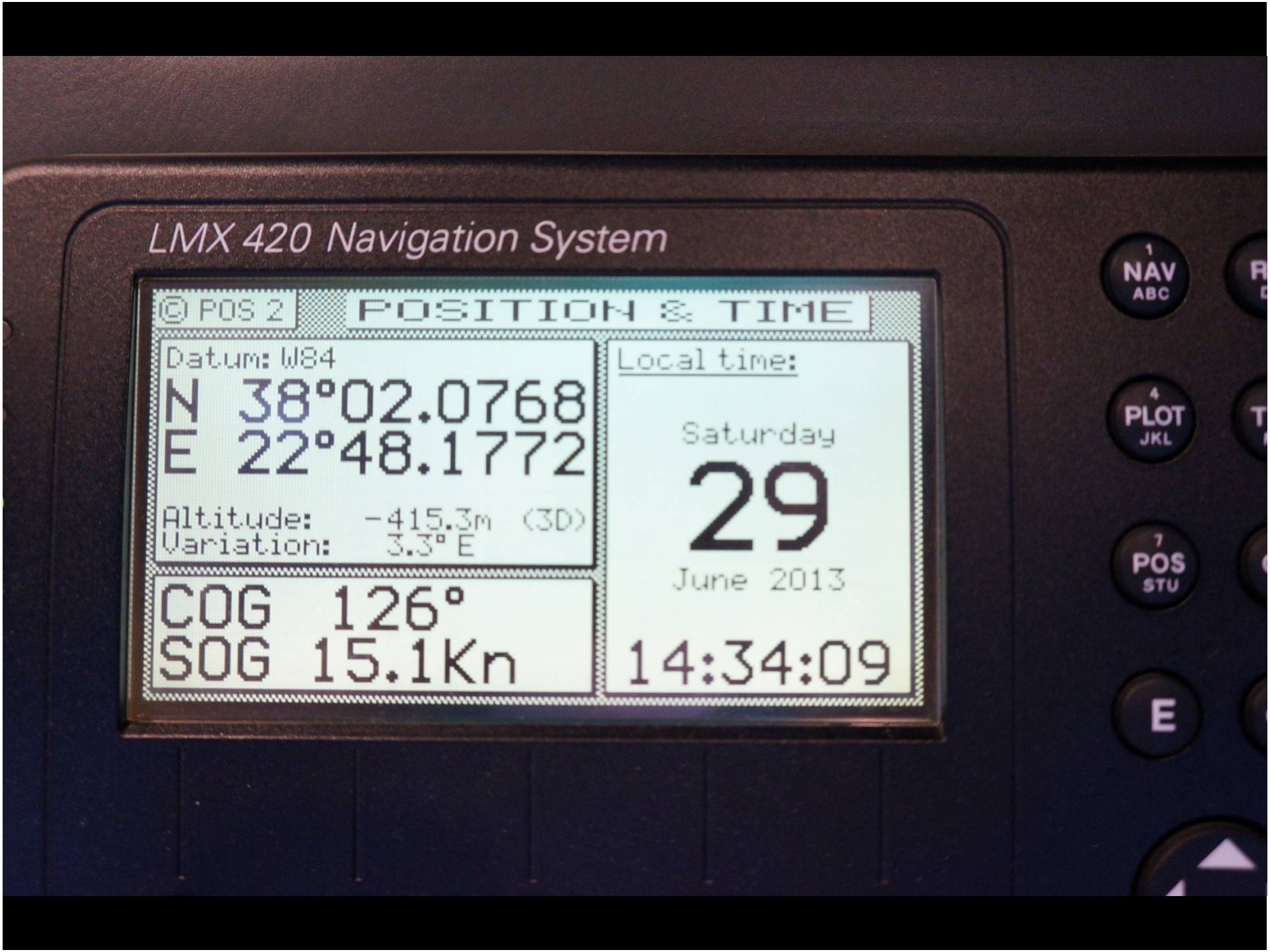

AUSTIN TX
MARCH 8–17
2013
SXSW
SXSW
MUSIC
FILM
INTERACTIVE


WHITE ROSE OF DRACHS


CERNIA
10nm
42°30N
42°25N
42°20N
10°45E
10°50E
10°55E
11°00E
LONE
Pta.Lividonia
Pta.Cala Grande
View
247621000
115.4°-41.6 nm
Pta.del
Fenaio
E1486 PUNTA FENAIO
PTA.DEL FENAIO
247102570
Old Lt Hc
Battery
SS
Mon
-496
P.del Giglio
ISOLA DEL GIGLIO
PROMONTORIO
ARGENTARIO
Pta.Faraglione
Restricted
Area
E1492 PUNTA DI CAPEL
PUNTA DEL CAPEL ROSSO
Pta.del Capel Rosso
1 : 100,000
ALARM
Sounder : no input
TRANSAS
Ship
26 - 06 . 13
01:00 E
06 : 52 : 32
Primary
42° 26.498 N
PS2:GPS
010° 44.552 E
COG-p
102.0°
SOG-p
15.0 kt
HDG-u
LOG-u
a1999
1 : 100,000
DANGEROUS SCALE
Route data
Route
Cap d'Ail to Bar 2013
To WP 3
CSE
115.4°
XTE
1.04 nm - stb
BTW
108.6°
DTW
8.79 nm
ETA (Ship)
26-06-2013 07:27:40
TTG
35 m 09 s
Next WP 4
CSE
149.2°
Radius
0.30 nm
Tasks List
Event
Help
Vectors
Fixed
Depth in Metres
WGS-84
Main
Dual
Add Info
AIS
Alarms
Charts
Config
Monitoring
NavTex
Route Planning
Targets
Tasks
MOB: CLICK THE LIFERING ICON ON THE BUTTON BAR


COSTA CONCORDIA

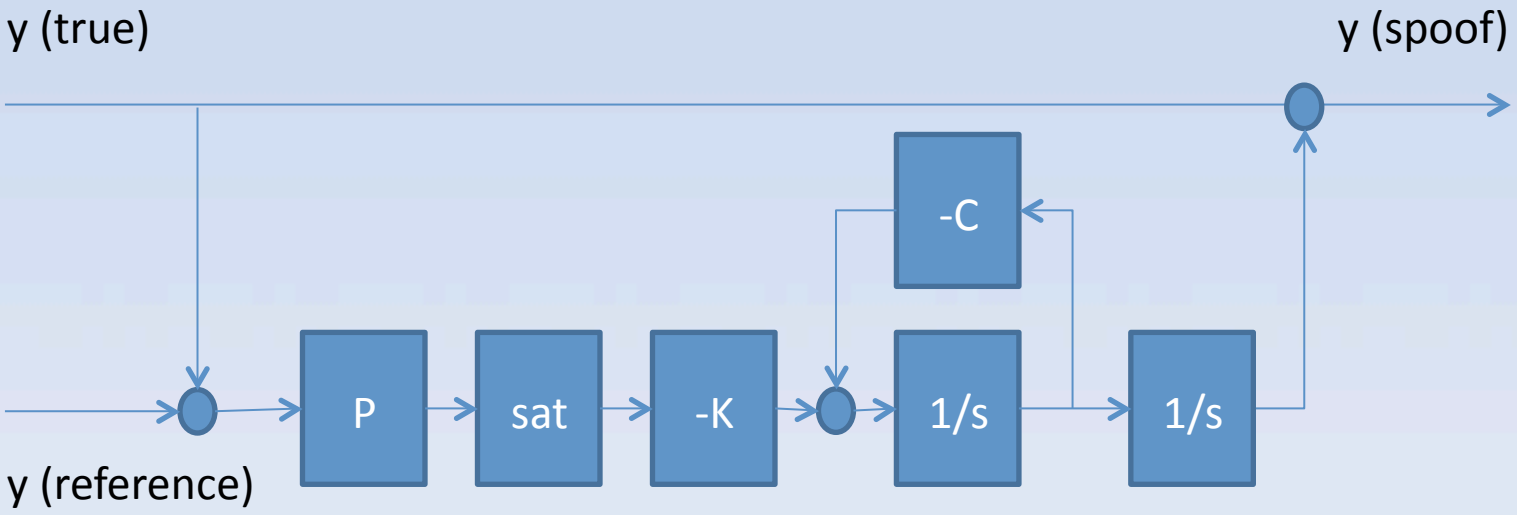

Panasonic


LMX 420 Navigation System
© POS 2
POSITION & TIME
Datum: W84
N 38°02.0768
E 22°48.1772
Altitude: -415.3m (3D)
Variation: 3.3° E
COG 126°
SOG 15.1Kn
Local time:
Saturday
29
June 2013
14:34:09
1 NAV ABC
4 PLOT JKL
7 POS STU
E

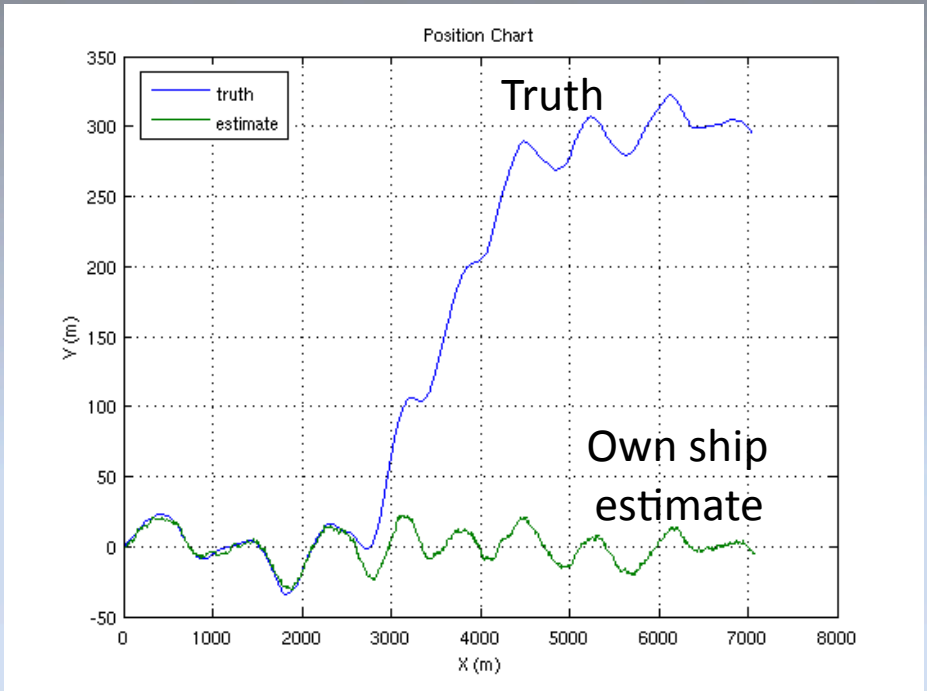

ARPA A
AIS
ALARM
Out of XTE
TRANSAS
Ship
29 - 06 - 13
03:00 E
17 : 57 : 11
Primary
37° 56.680 N
PS2:GPS
022° 58.350 E
COG-p
126.0°
SOG-p
6.6 kt
HDG-u
LOG-u
N UP
H UP
C UP
RM
TM
1:1
gr232_2
1 : 15,000
Route data
Route
Bar to fethiye 2013
To WP 15
CSE
132.3°
XTE
139 m - port
BTW
134.0°
DTW
2.56 nm
ETA (Ship)
29-06-2013 18:20:27
TTG
23 m 17 s
Next WP 16
CSE
121.6°
Radius
0.30 nm
Tasks List
Event
Help
Vectors
Fixed
Show
Depth in Metres
WGS-84
LATERAL BUOYAGE
KORINTHOU CANAL
Isthmia
Sinking Bridge
gr232_2d
1 : 15,000
Main
Dual
Add Info
AIS
Alarms
Charts
Config
Logbook
Monitoring
NavTex
Route Planning
Tasks
MOB: CLICK THE LIFERING ICON ON THE BUTTON BAR

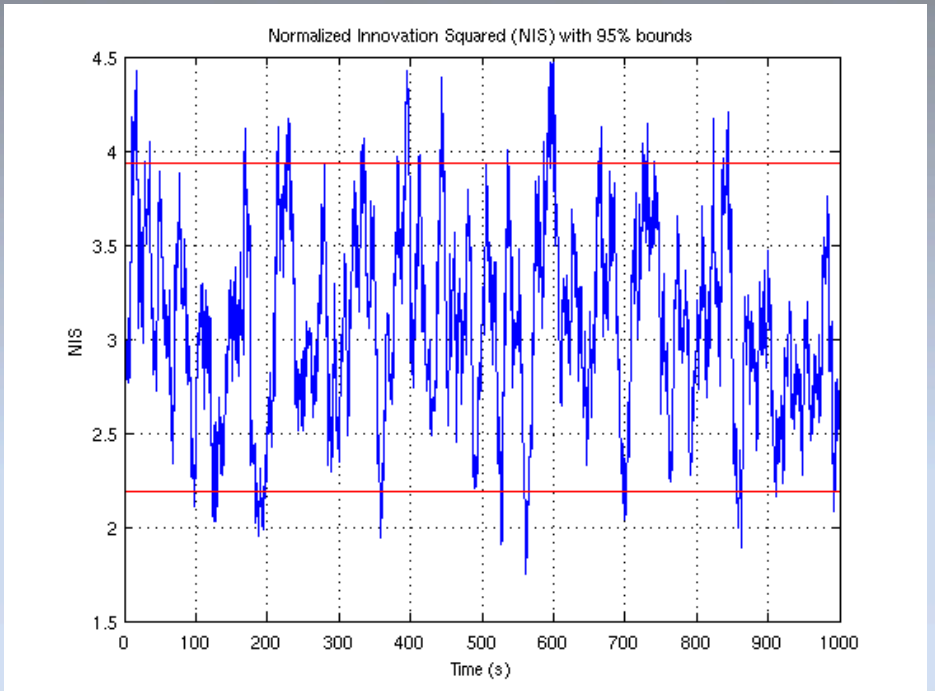
Covert Post-Capture Ship Control

If the spoofer has an estimate of the rhumb line that the ship is following, then the spoofer can employ a saturating PD controller to covertly force the ship to track a reference cross-track position



Covert Post-Capture Ship Control

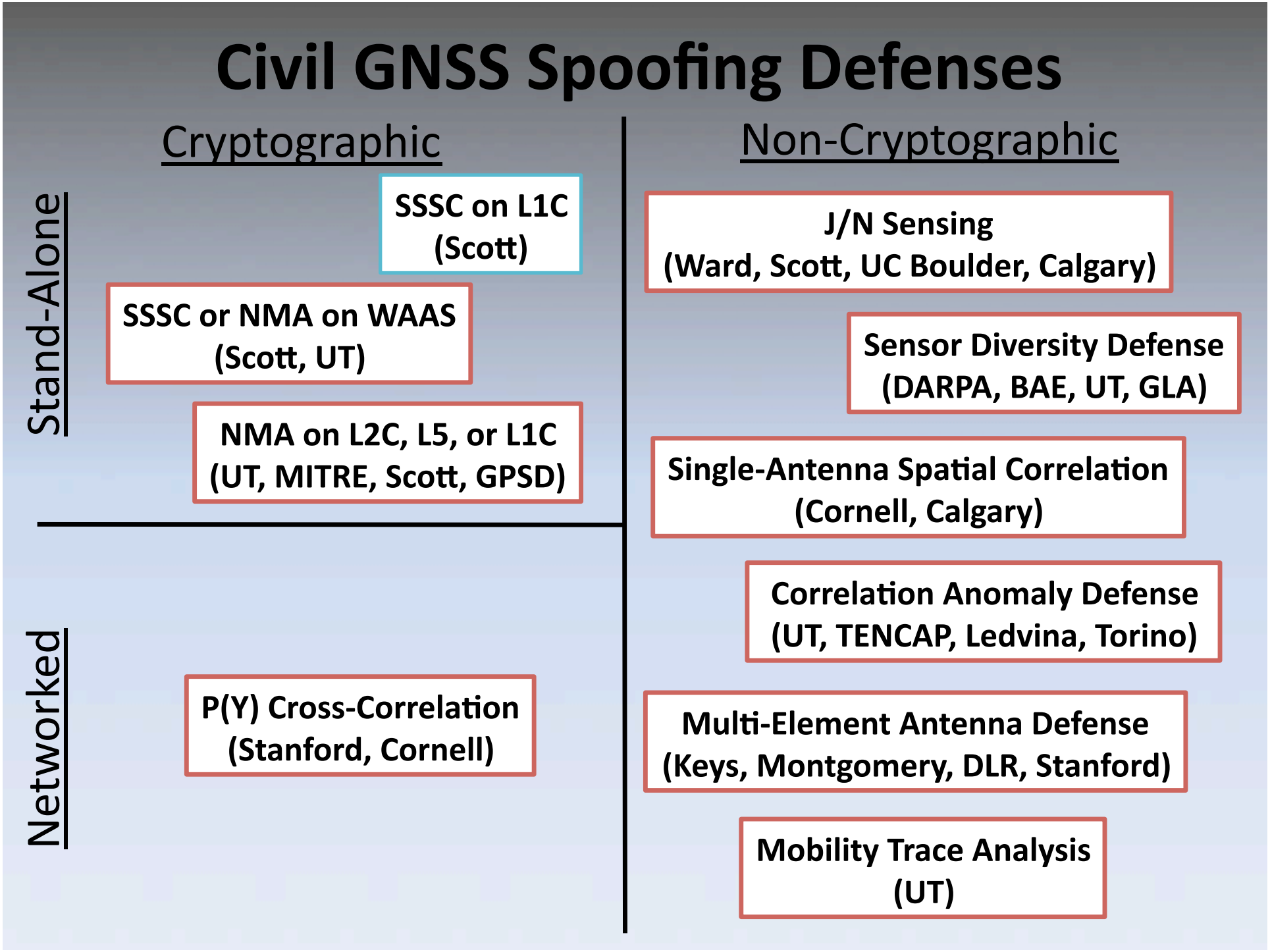




No alarms triggered by Chi-square-type test

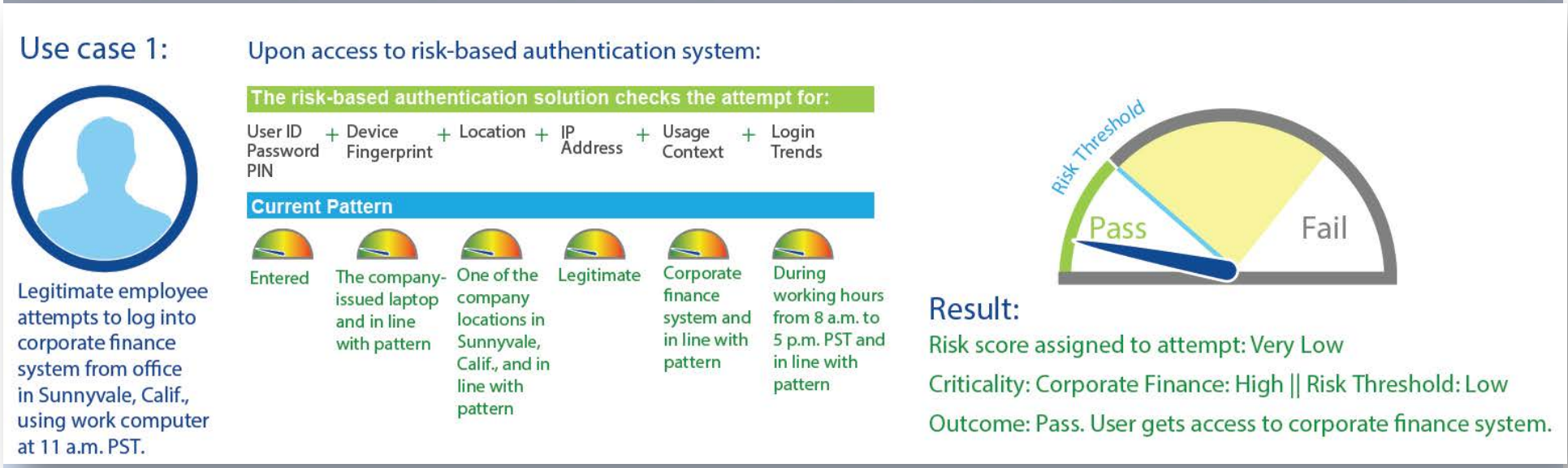
Stable covert post-captue ship control is possible provided the spoofer can estimate the ship's rhumb line

Civil GNSS Spoofing Defenses



The greatest challenge in PNT security will be providing *proof of location or time* to a skeptical second party. This problem *scales differently* than attacks against non-complicit PNT sensing: A single rogue actor with an inexpensive receiver network ("Dr. No") could sell forged GNSS-based proofs of location and time to thousands of subscribers. Such subversion may not even be illegal ...

Beyond the Password:
Risk-Based User Authentication:

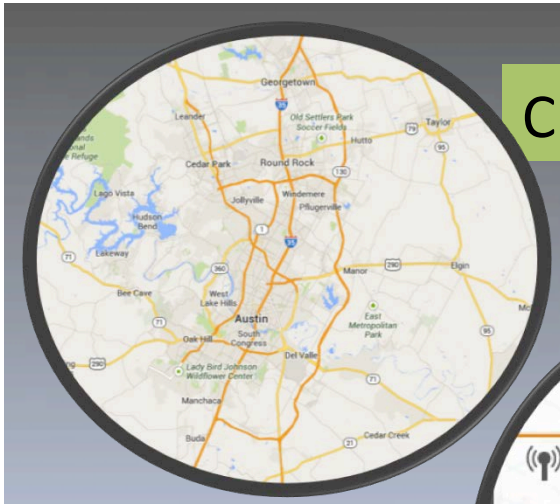


Graphic courtesy Deloitte/WSJ

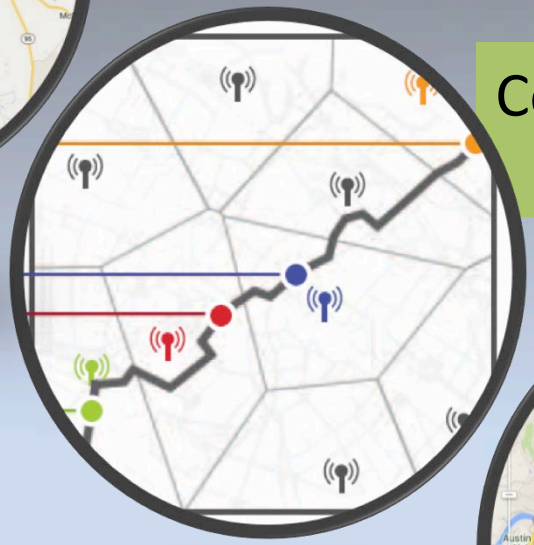
Trustworthy proof of location is central to risk-based user authentication

Mobility Trace Analysis

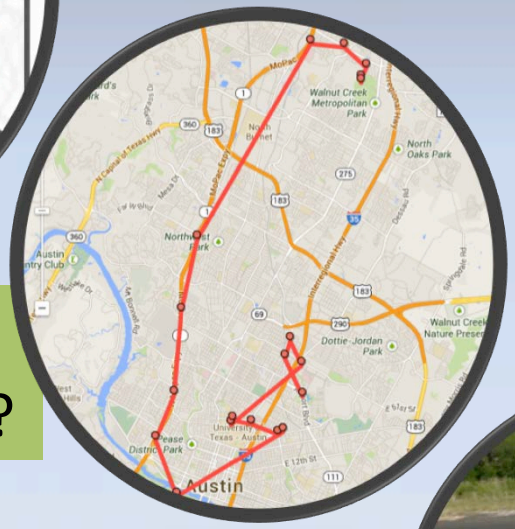
City-level: Where do you live?



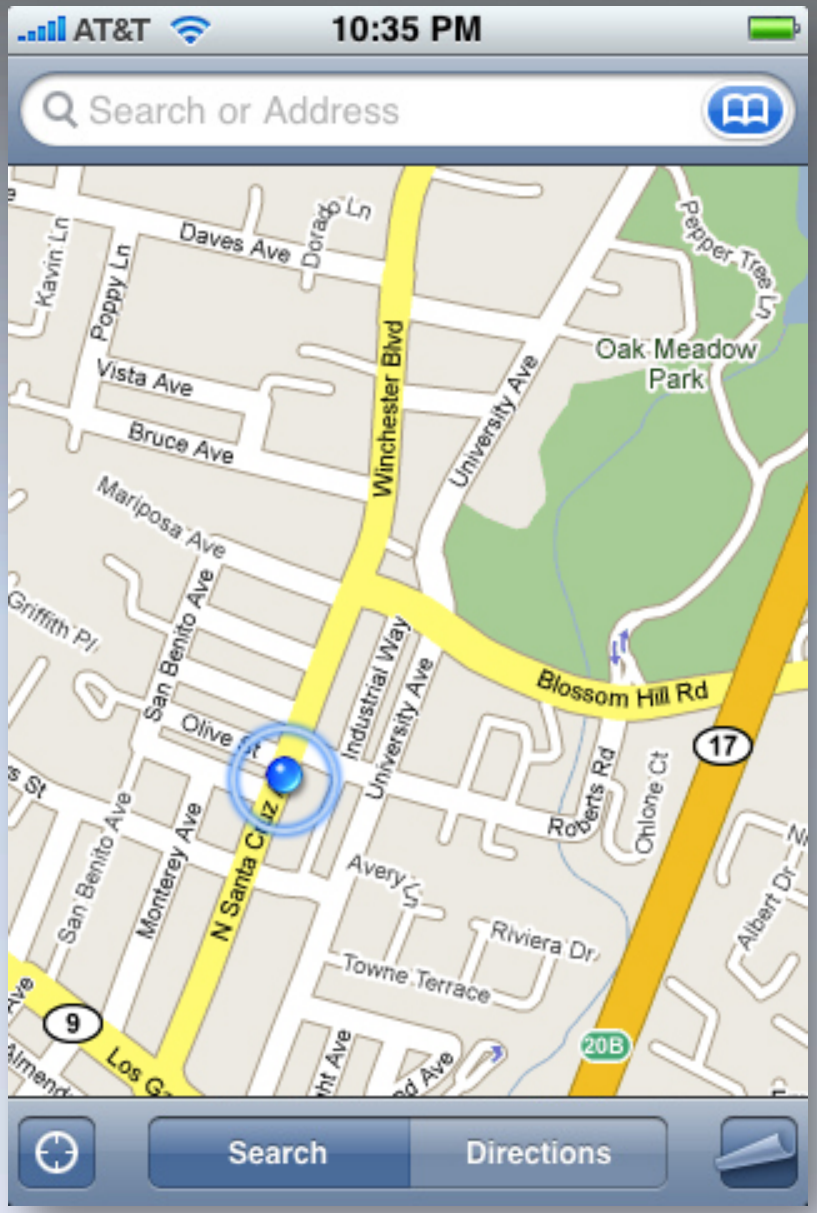
Cell-level: What are your daily patterns?



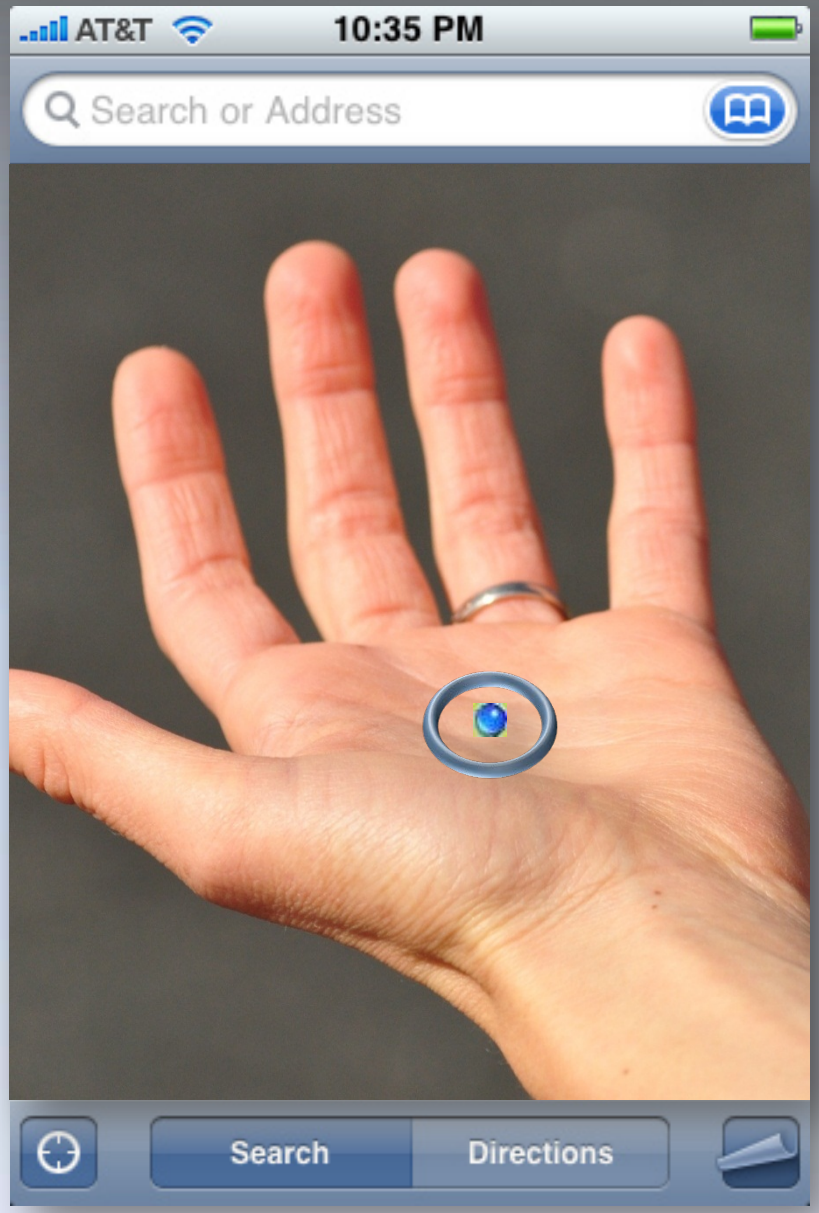
Coarse GPS/WiFi-level:
On what street are you travelling?

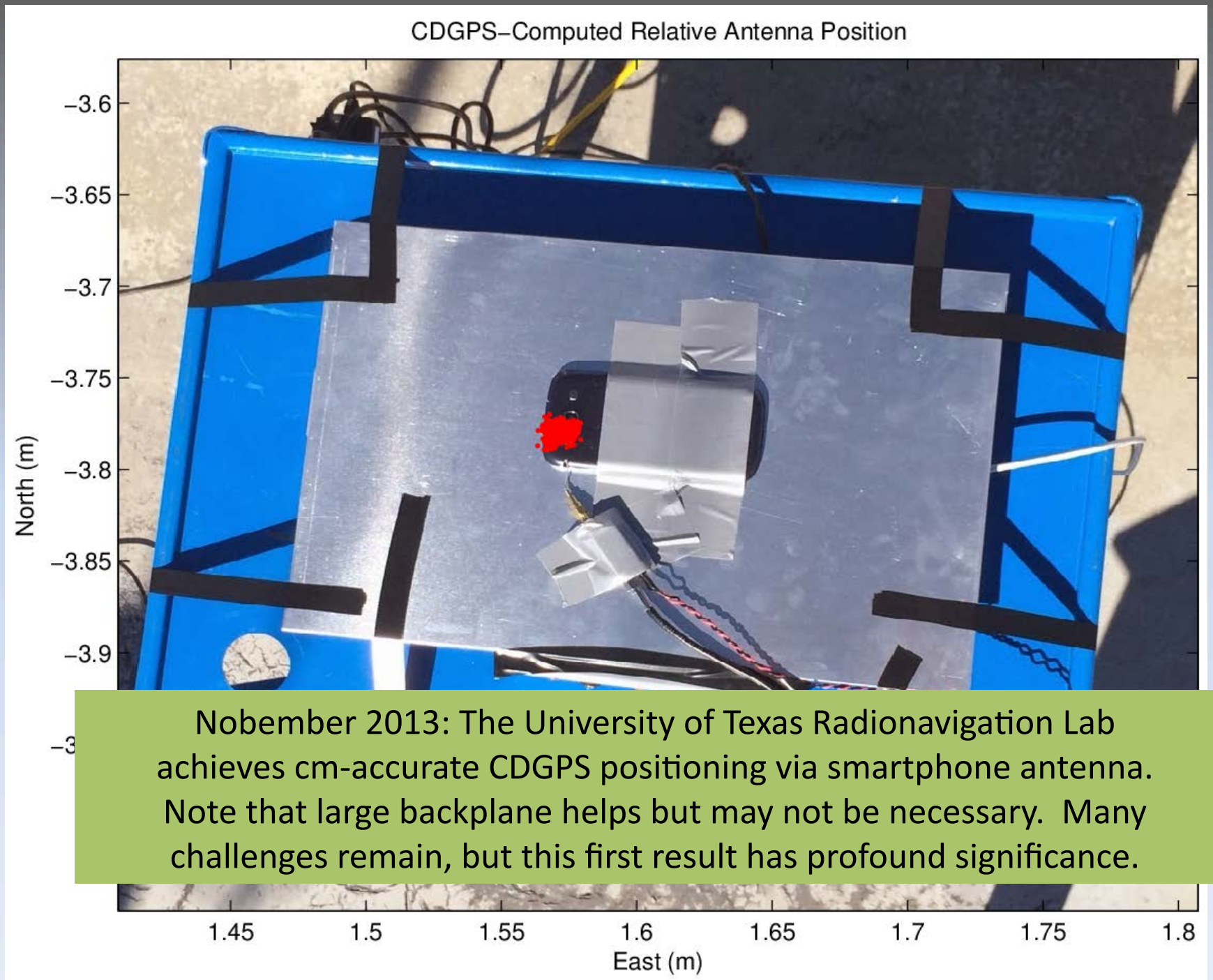


Decimeter-level:
Are you driving unusually today?

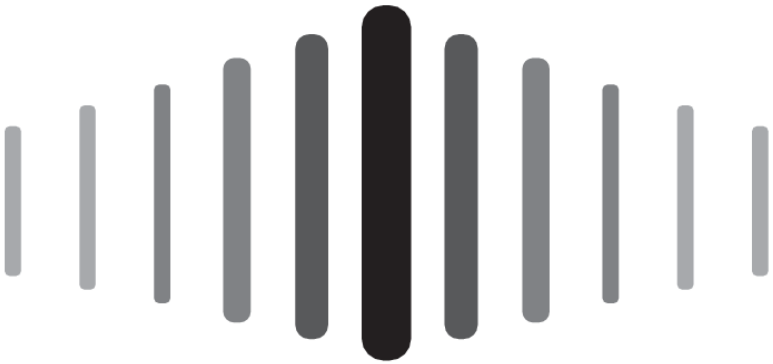

AT&T
10:35 PM
Search or Address
Daves Ave
Dorado Ln
Kavin Ln
Poppy Ln
Vista Ave
Bruce Ave
Mariposa Ave
Winchester Blvd
University Ave
Pepper Tree Ln
Oak Meadow Park
Griffith Pl
San Benito Ave
Olive St
Industrial Way
University Ave
Blossom Hill Rd
17
Roberts Rd
Ohlone Ct
Albert Dr
Monterey Ave
N Santa Cruz
Avery St
Riviera Dr
Towne Terrace
9
20B
Search
Directions


AT&T
10:35 PM
Search or Address
North Santa Cruz Avenue / Olive Street
© 2011 Google
Search
Directions


AT&T
10:35 PM
Search or Address
Search
Directions



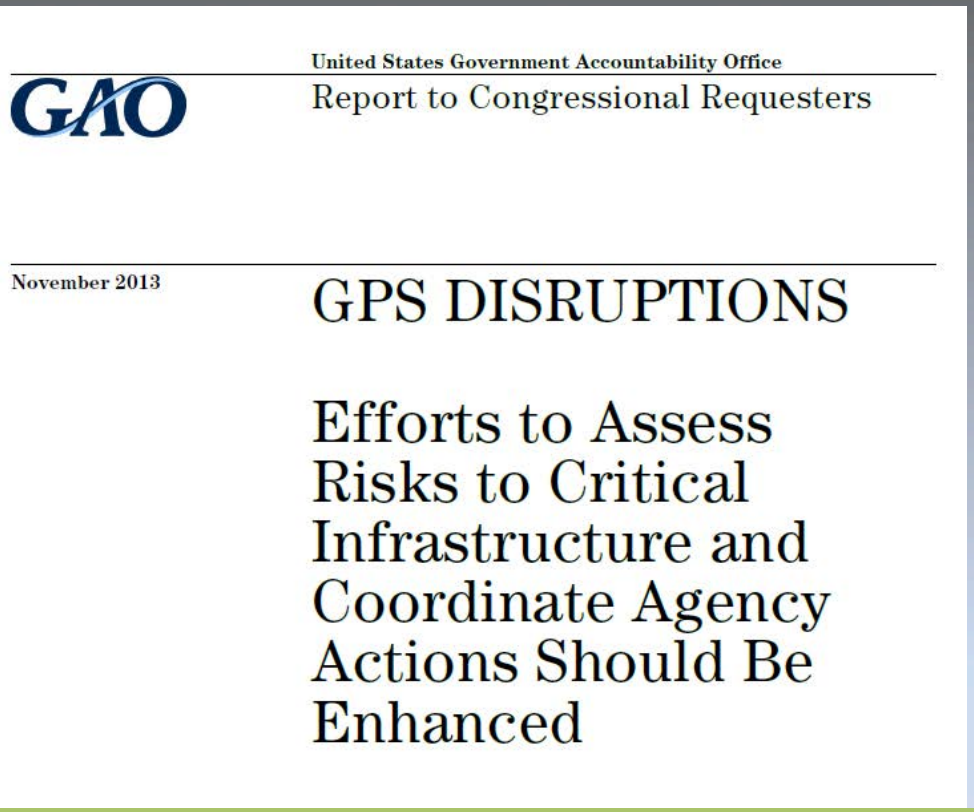
Nobember 2013: The University of Texas Radionavigation Lab achieves cm-accurate CDGPS positioning via smartphone antenna. Note that large backplane helps but may not be necessary. Many challenges remain, but this first result has profound significance.



THE UNIVERSITY OF TEXAS AT AUSTIN

RADIONAVIGATION LABORATORY

radionavlab.ae.utexas.edu


United States Government Accountability Office

GAO

Report to Congressional Requesters

November 2013

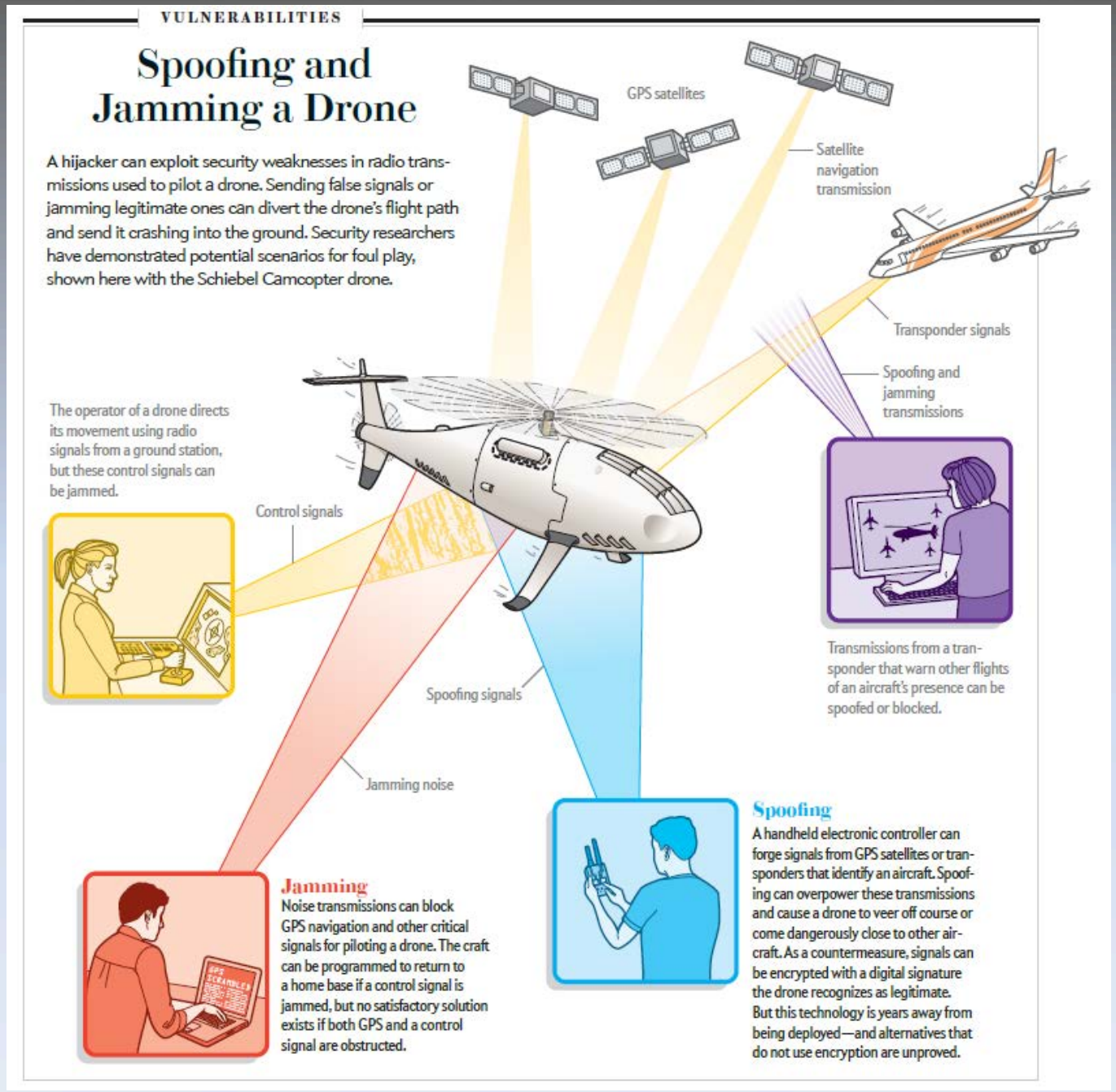
GPS DISRUPTIONS

Efforts to Assess Risks to Critical Infrastructure and Coordinate Agency Actions Should Be Enhanced

GAO-14-15

"[D]ue to resource constraints and other reasons, the [DHS and DOT] have made limited progress in meeting [NSPD-39], and many tasks remain incomplete, including identifying GPS backup requirements and determining suitability of backup capabilities."

"[O]verall, the requirements of NSPD-39 remain unfulfilled."



Wesson and Humphreys, Scientific American, Nov. 2013

Questions on Marine Spoofing (1/2)

- *Does the attacker have to be aboard the target vessel?* No. We launched the attack from onboard the WROD only for convenience. So long as the target's approximate position is known, the attacker can be miles away.
- *Won't there be a discrepancy between the gyrocompass heading and the GPS-produced Course Over Ground?* Yes, but a subtle spoofer can make a small heading offset look like the effect of an ocean current.

Questions on Marine Spoofing (2/2)

- *Wouldn't GPS deception be revealed by a consistency check between radar returns and objects on the ECDIS?* Quite possibly. This cross-check is a valuable defense. But it's not much use in the open seas, and, sadly, maritime radar can be spoofed too.
- *But I could simply use a sextant and a clock to determine my location, true?* Yes, but what's sinister about GPS deception is that you probably won't *know* you're being spoofed. And a sextant isn't accurate to better than a few nm. And do you remember how to work it?