Logan Scott, President, LS Consulting
www.gpsexpert.net

The Role of Civil Signal Authentication in Trustable Systems

Presentation to:
59th CGSIC Plenary, 17 September 2019, Miami Florida

Logan Scott has over 35 years of military and civil GPS systems engineering experience. He is a consultant specializing in radio frequency signal processing and waveform design. At Texas Instruments, he pioneered approaches for building high-performance, jamming-resistant digital receivers.

At Omnipoint (now T-Mobile), he developed spectrum sharing techniques that led to a Pioneer's preference award from the FCC. He is a cofounder of Lonestar Aerospace, an advanced decision analytics company located in Texas.

Logan has been an active advocate for improved civil GPS location assurance through test based GPS receiver certification, crowdsourced jammer detection and location, and, by adding robust signal authentication features to civil GPS signals. He is currently consulting with AFRL on waveforms for advanced navigation capabilities.

Logan is a Fellow of the Institute of Navigation and a Senior Member of IEEE. In 2018 he received the GPS World Signals award. He holds 43 US patents.

In a Critical Application Which Would You Prefer?

- A GNSS receiver that provides position and time
  A. in real time BUT with limited assurance

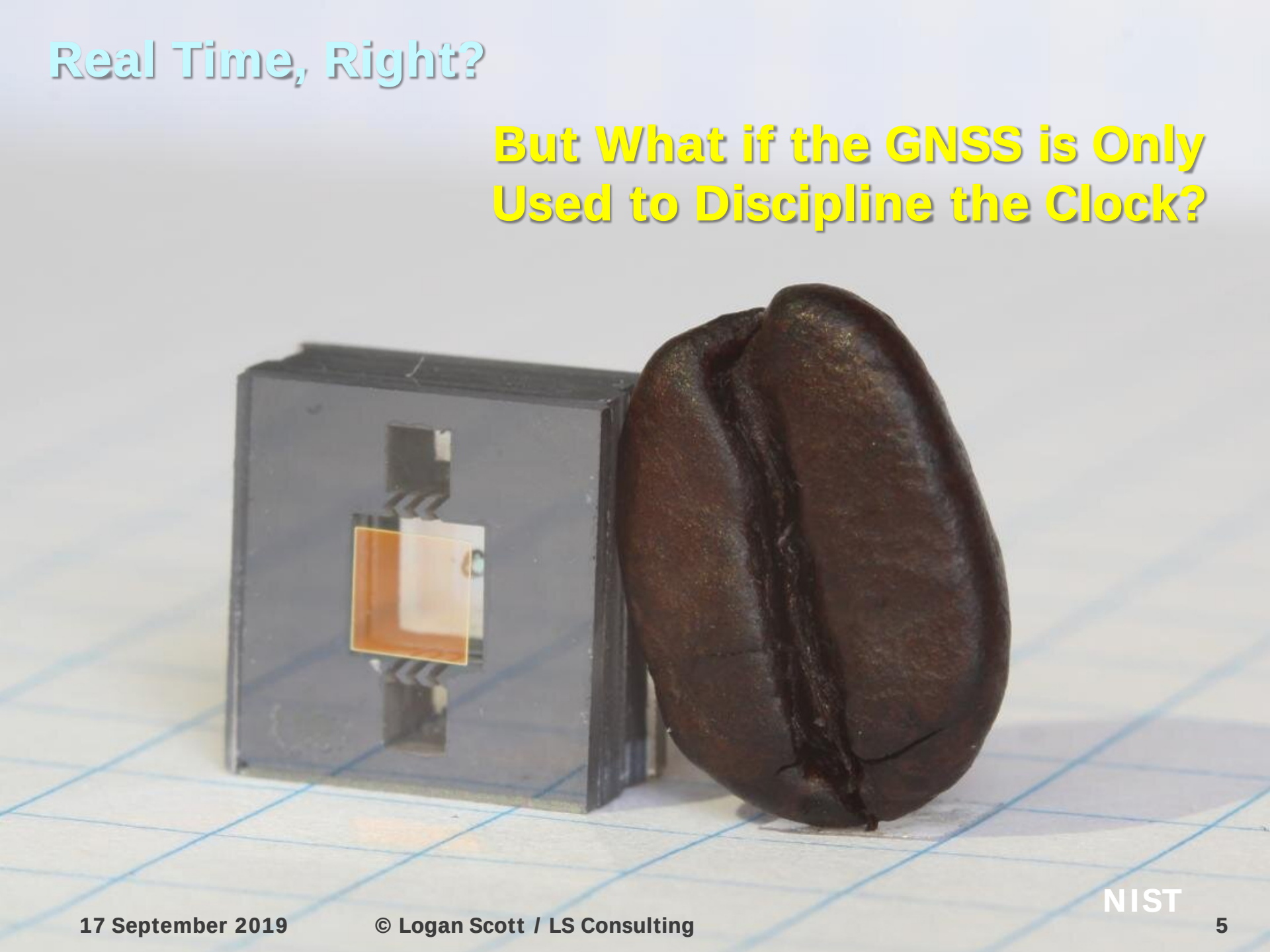
  B. with very high assurance BUT with a 6 second delay
     - delay is known to within a few nanoseconds

Real Time, Right?

But What if the GNSS is Only Used to Align the Inertial?

Real Time, Right?

But What if the GNSS is Only Used to Discipline the Clock?



Real Time, Right?

Real Time, Right?

A 6 second delay might be preferable

- **Corrupt GNSS can drive a clock or IMU into an irredeemable error state or prevent TERCOM acquisition**
- GNSS / Clock
  - GNSS disciplines the clock's drift errors
- GNSS / IMU (inertial measurement unit)
  - GNSS disciplines the IMU's error states
- GNSS / Autonomous
  - GNSS initializes TERrain COMparison (TERCOM) processes

Trust takes Time and Memory

A Fundamental Shift in PVT Security Paradigms

- With a 6 second delay, a GNSS receiver has time to ponder
  - It can look at trends in quality metrics without having to make real-time judgments
  - In a sense, receiver algorithms can look 6 seconds into the "future"
- With a 6 second delay, a GNSS receiver can withhold judgment until all the facts are in
  - Did that signal originate from a GPS satellite?
  - Are the watermarks in the right place, at the right power?

IS-AGT-100 Defines an Experimental , Backwards Compatible Security Overlay for the L1C Civil Signal Embodies Most Concepts from my 2003 and 2013 papers

- Message Signing
- Fast & Slow Watermark Channels
  - 6 second epoch
  - 3 minute epoch

This is an NTS-3 Capability

IS-AGT-100
17-APR-2019

AIR FORCE RESEARCH LABORATORY
SPACE VEHICLES DIRECTORATE
ADVANCED GPS TECHNOLOGY

INTERFACE SPECIFICATION
IS-AGT-100

Chips Message Robust Authentication (Chimera) Enhancement for the L1C Signal: Space Segment/User Segment Interface

APPROVED BY:

Digitally signed by CHAPMAN.DAVID.C.1392891761
Date: 2019.04.17 16:49:32 -06'00'

David C. Chapman, DR-03, DAF
Program Manager
Advanced GPS Technologies Program

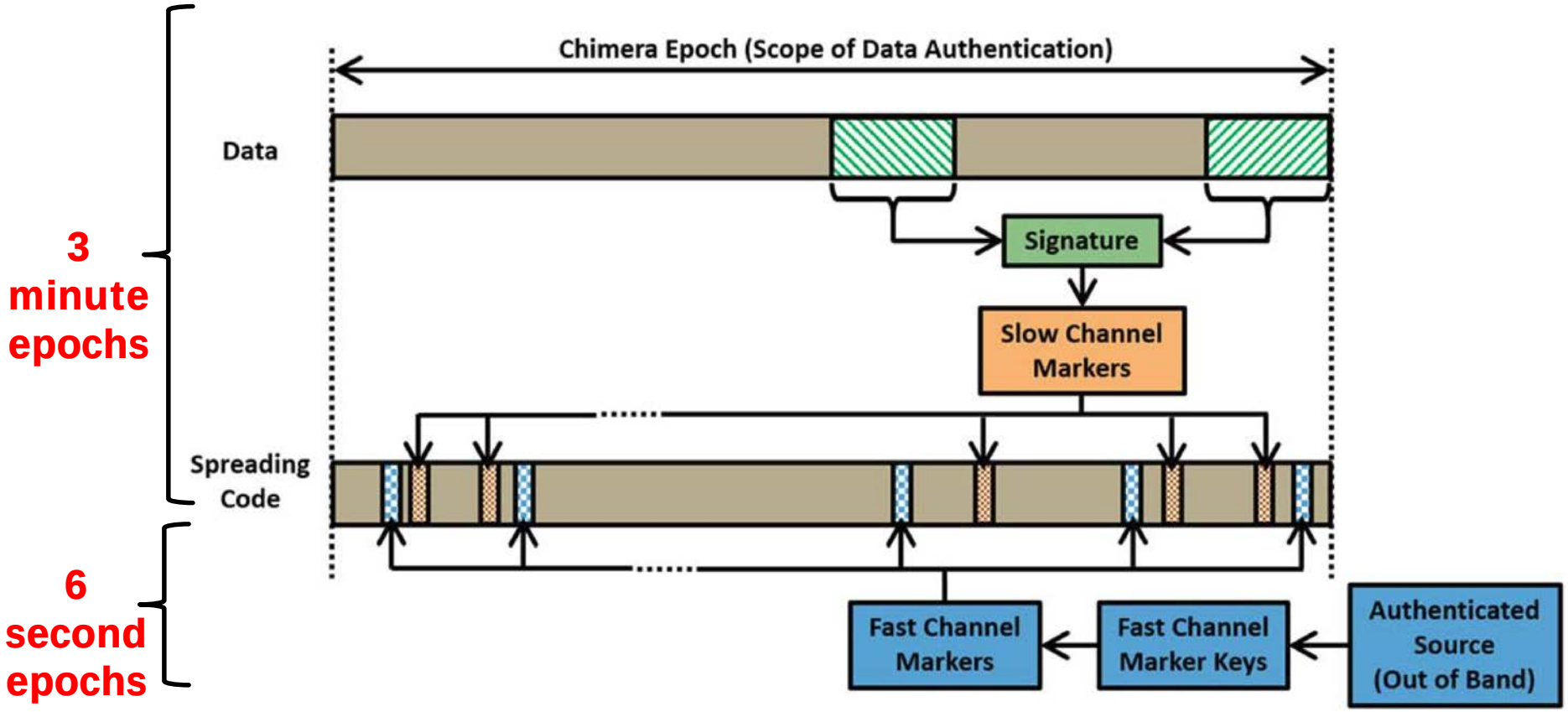
Date

DISTRIBUTION STATEMENT A. Approved for Public Release; Distribution is Unlimited

Signal Specification and Select Papers are at
http://www.gpsexpert.net/chimera-specification

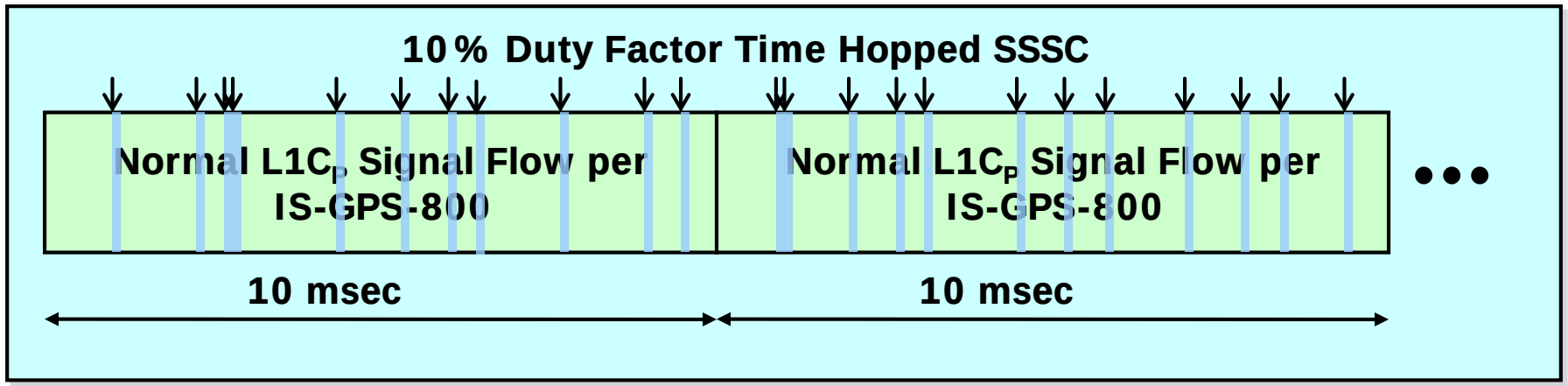
CHIMERA Signs Data Messages

ECDSA P-224 Signature Is Hashed to Create the Slow Channel Marker Generation Key



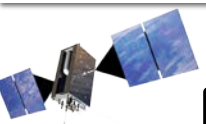
From IS-AGT-100

Watermarking Signals with Spread Spectrum Security Codes (SSSC) Can Establish Provenance



- Watermark Generating Key Determines Security Code Values AND Insertion Locations
  - Key Is Changed Once Every 3 minutes
- Key is Published to The User Segment ONLY After Key Has Changed
  - Published By Satellites & via Secure Server
  - Secure Key Storage IS NOT Required in User Equipments
- The Watermark Is Hard To Forge
  - Spoofer/Forger Has to Read SSSC Chips Off The Air

Apriori Receiver Time Uncertainties and Marker Generation Key Time of Publication Determines Which Markers Can Be Used in Authentication



Satellite

Marker Key_{N-1} Used To Generate Markers	Marker Key_N Used …

Receiver

Marker Key N-1 Published

Markers Potentially Collected By Receiver	
Adversary Could NOT Have Had Marker Generating Key *(OK to Use These for Authentication)*	Adversary Could Have Had Marker Generating Key

Receiver Knows Time to Be In This Range

Time

With 10% Watermarks, You Can Still Track The Signal In Real Time

Less Secure Receivers Can Ignore Watermarks

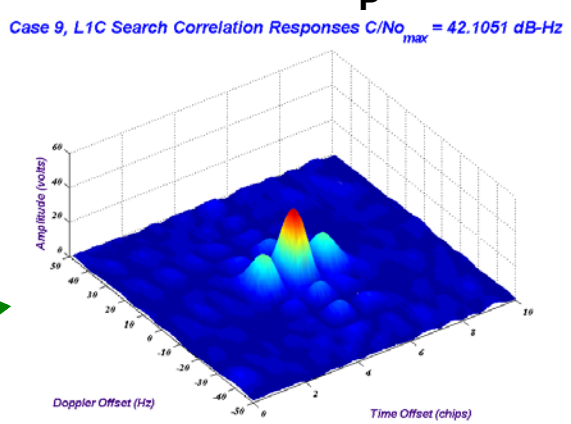
The Transmitted Signal Has 3 Channels

- Pilot
- Data (Signed)
- SSSC

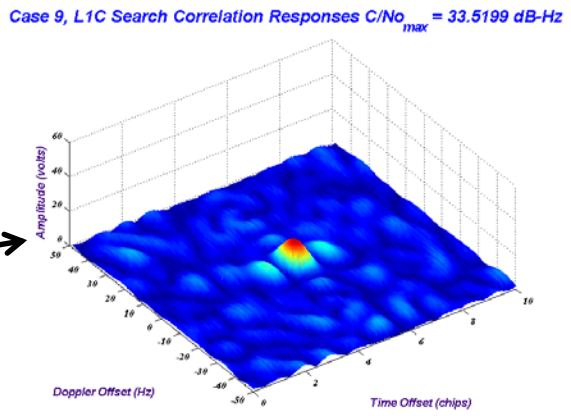
Real Time
No Key Needed

Need Watermark Key

Rx:L1C$_P$



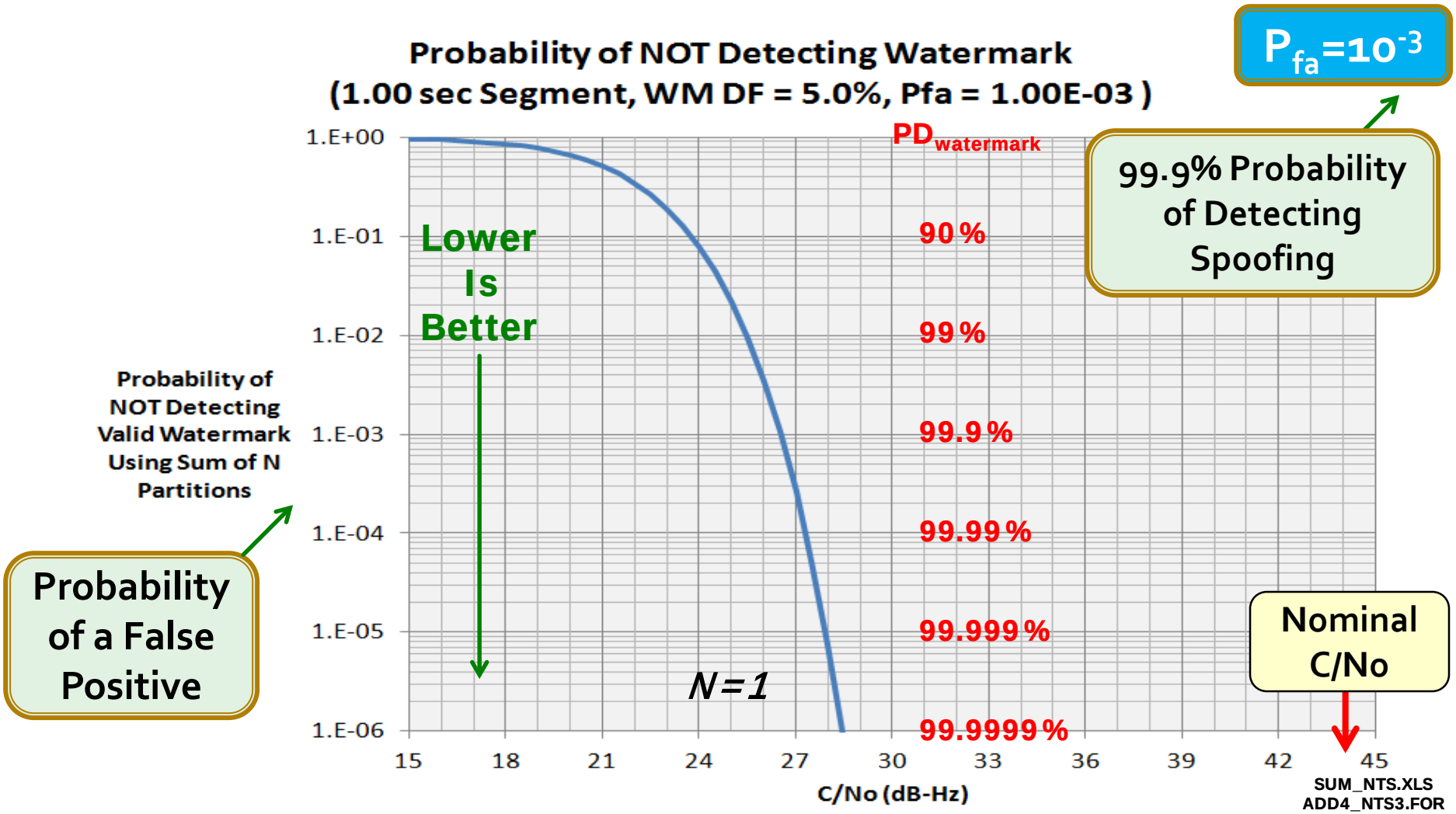
Rx: SSSC



If You Don't See This Aligned to the Pilot, The Signal Didn't Come from a GNSS Satellite

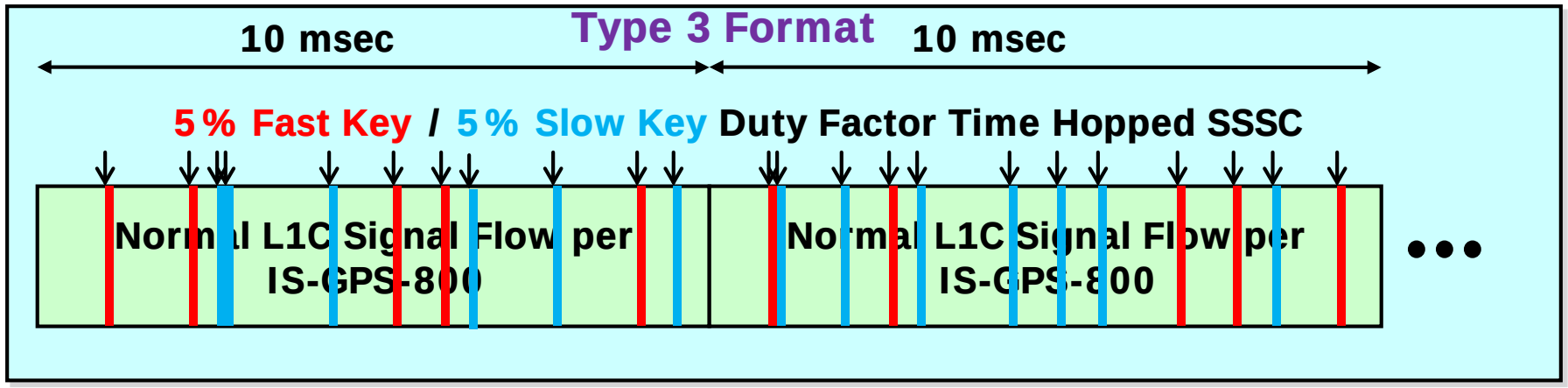
Watermarks Provide an Extremely Low False Positives Rate and a High Probability of Detecting Spoofing

Declaring SPOOFING is Like Yelling FIRE in a Crowded Theatre!



Fast Key (6 Second) and Slow Key (3 minutes) SSSC Streams Support Diverse User Communities

- **Fast Keys** Change Every 6 Seconds
  - Keys Obtained via Authenticated Out of Band Channel (e.g. Internet)
  - Low Latency Authentication / PoL with Fast Update Rate
- **Slow Keys** Change Every 3 Minutes
  - Keys Transmitted By GNSS Satellite for Standalone Capability
  - Provides Bootstrap into Using Fast Channel if Initial Time Uncertainty is Large



There are a Lot Of Methods for Detecting RF Spoofing
Many Can Be Manipulated to Create False Positives DoS

Anti-Spoofing Method	Spoofing Feature	Complexity	Effectiveness	Receiver Required Capability	Spoofing Scenario Generality
RSS Monitoring	Higher C/N0	Low	Medium	C/N0 Monitoring	Medium
RSS Variation vs. Receiver Movement	Higher Power Variations due to proximity	Low	Low	Antenna Movement / C/N0 Monitoring	Low
Antenna Pattern Diversity	Low elevation angle	Medium	Medium	Special Designed antennas	Medium
L1/L2 Power Comparison	No L2 Signal for Spoofer	Medium	Low	L2 Reception Capability	Medium
Direction of Arrival Comparison	Spoofing signals Coming from the Same Direction	High	High	Multiple Receiver Antennas	High
Pairwise Correlation in Synthetic Array	Spoofing signals come from the Same Direction	Low	High	Measuring Correlation Coefficient	High
TOA Discrimination	Inevitable Delay of Spoofing Signal	Medium	Medium	TOA Analysis	Low
Signal Quality Monitoring	Deviated shape of Correlation Peak	Medium	Medium	Multiple Correlators	Low
Consistency Check with other Solutions	Inconsistency of Spoofing Solution	High	High	Different Navigation Sensors	High
Cryptographic Authentication	Not Authenticated	High	High	Authentication	High
Code and Phase rate Consistency Check	Mismatch between Spoofed Code and Phase rate	Low	Low	---	Low
GPS Clock Consistency	Spoofing/Authentic Clock Inconsistency	Low	Medium	---	Medium
Multiple Receiver Spoofing Detection	Same Solution for Different receivers/absence of valid spoofed P(Y)	Medium	High	Data link Between Receivers	High

RECEIVERS ARE COMPUTERS AND ARE SUBJECT TO CYBER ATTACK

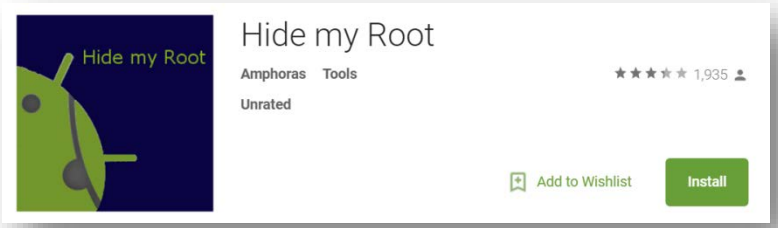
WATERMARKING CAN AID IN DETECTION

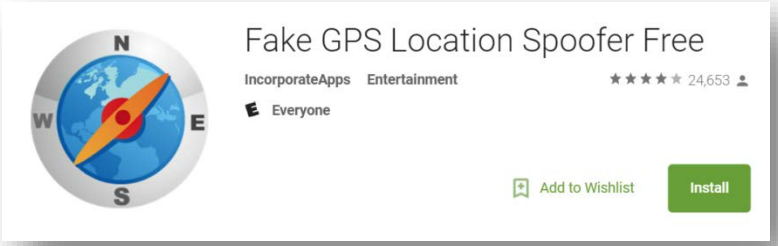
Table from: Ali Jahromi PhD Thesis, *GNSS Signal Authenticity Verification in the Presence of Structural Interference*, UCGE Reports Number 20385, 2013

Two Ways to Cheat at Pokémon Go

Hint: Method 1 Costs Less and is More Reliable

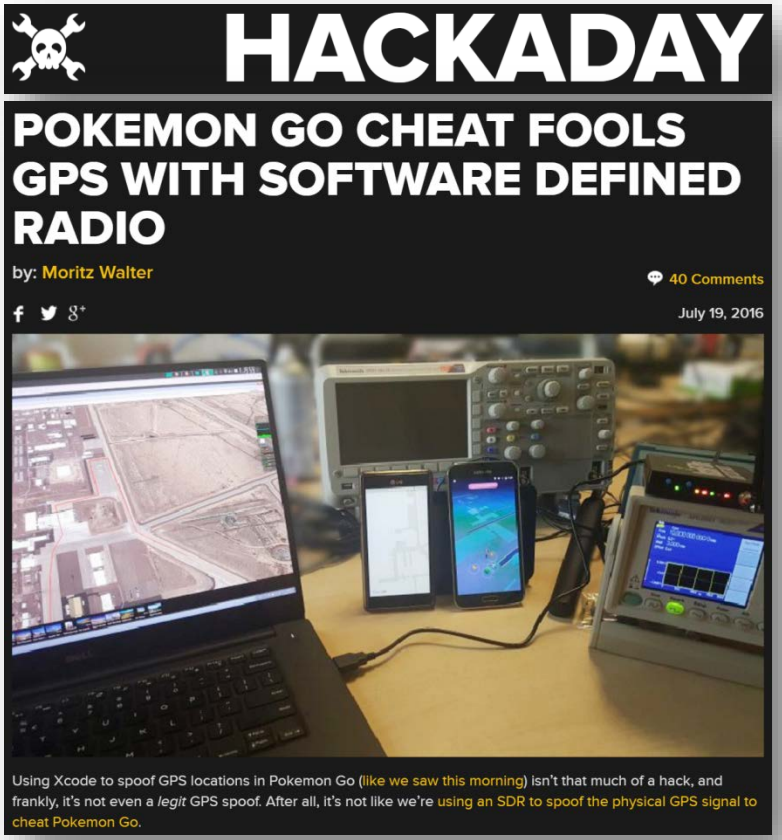
Method 1





This is a Man in the Middle Attack

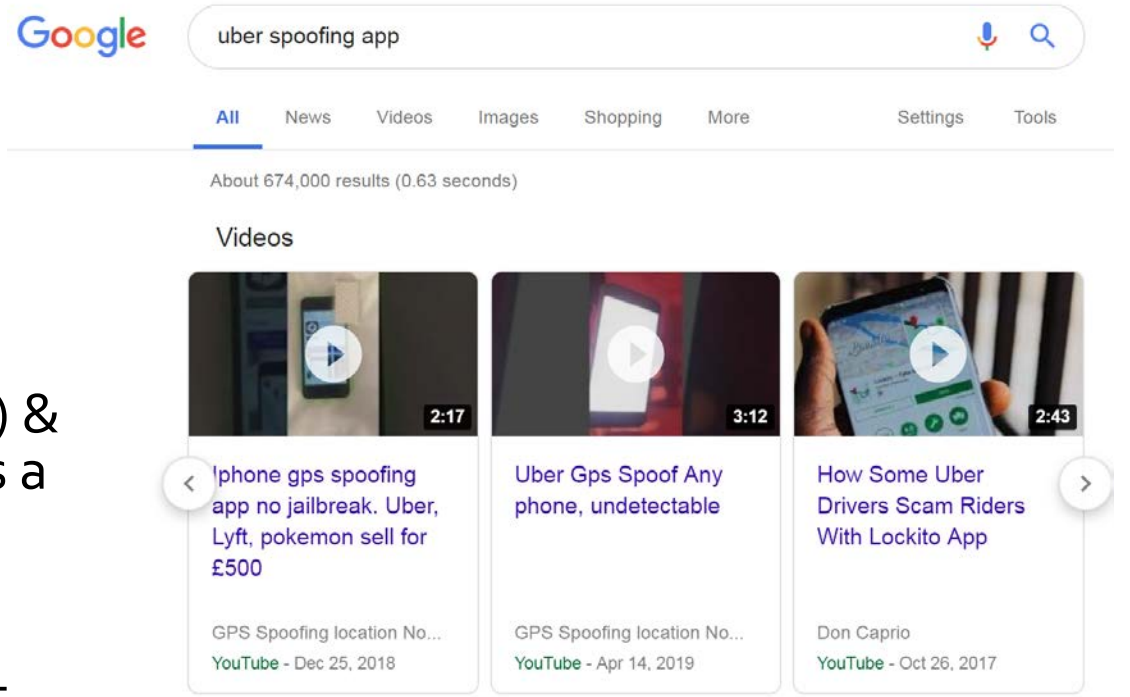
Method 2



Monetizing Location Spoofing By Becoming a Virtual Ridesharing Driver

Pokémon Go was an early example of a new style of exploit

1. Sign Up to Be a Driver using Stolen ID
2. Install Location Spoofer App
3. Obtain OP Credit Card(s) & Identities and Sign Up as a Rider(s)
4. Accept Rides in Virtual Space and Get Paid for it



Scale Up by Renting a Botnet or Hire some Smurfs

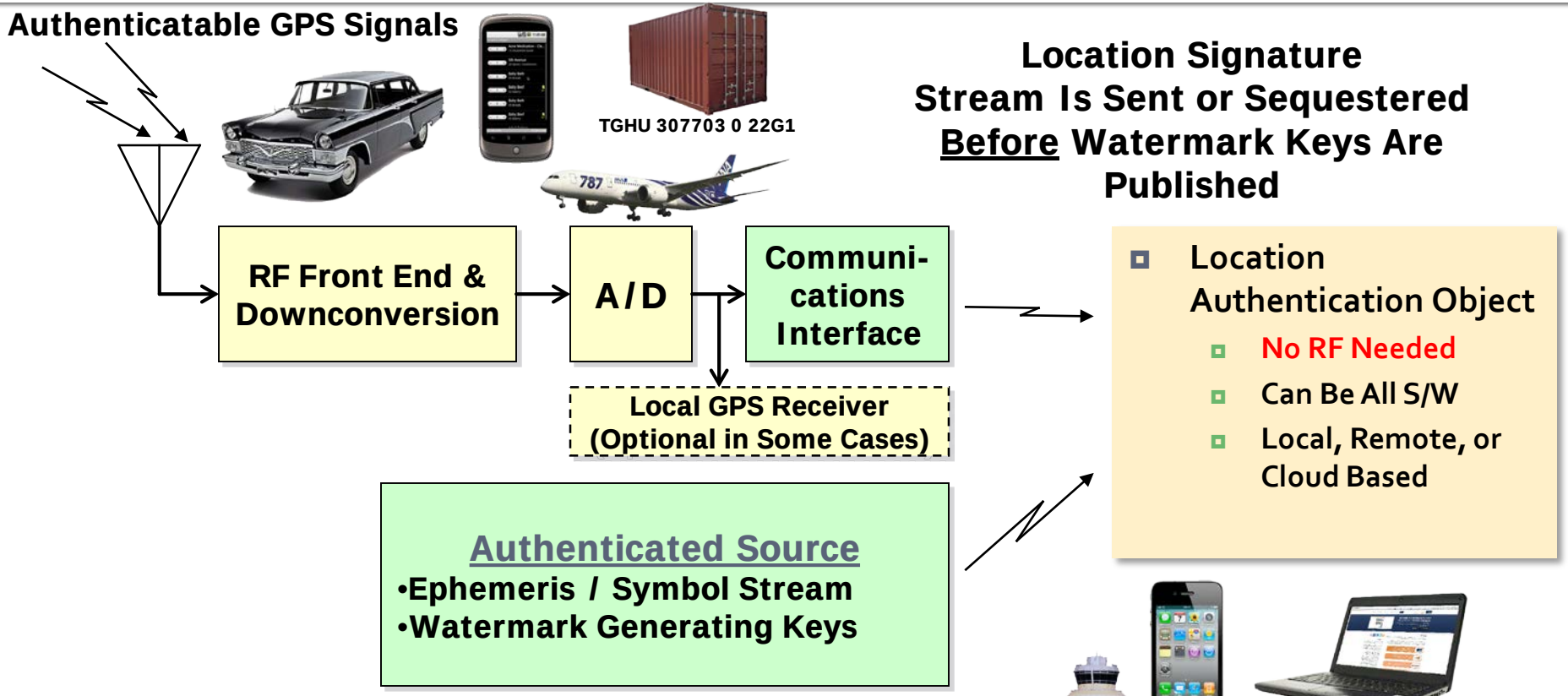
Spoofing Is an Effect, Not a Method

- Cyberspoofing Is Oftentimes a More Effective Method
  - Can Be Used to Corrupt Databases with Location Dependent and/or Crowdsourced Entries
    - Traffic Estimates
    - The US Census
  - Can Bias Conclusions Drawn from the Database
    - Where Traffic Flows
    - Where Money Flows

- **Watermarking Can Play an Important Role in Detecting Location Spoofing By Providing Location Signatures**

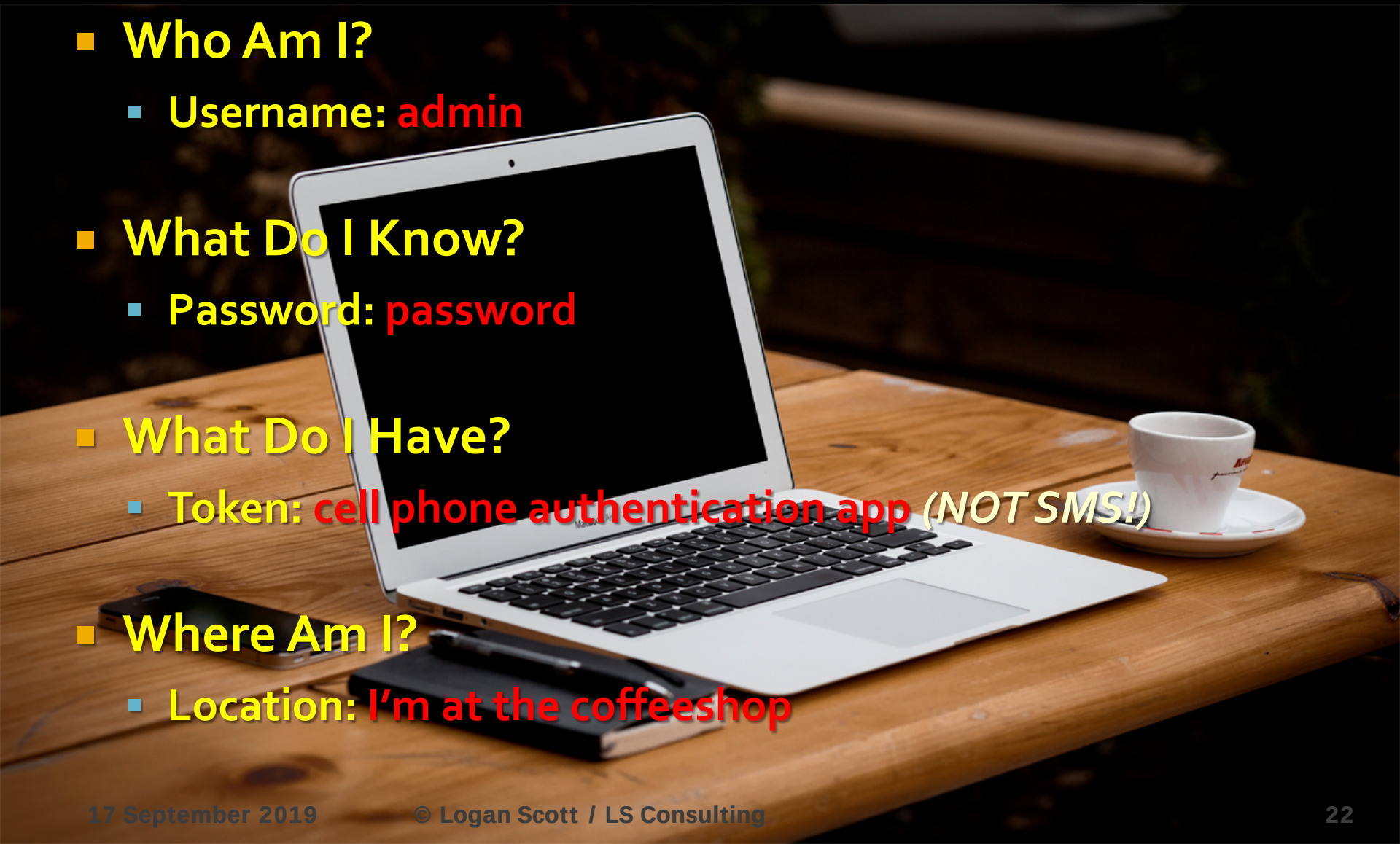
Proofs of Location Check For Valid Watermarks etc.

Less Trust in the Sender and Intervening Comms



- Location Signature is ~125 Kbyte (Nominal)
- Diverse Trust Models Are Possible

IF Location Is Trustable, Information Access & Permissions Can Include Location Factors



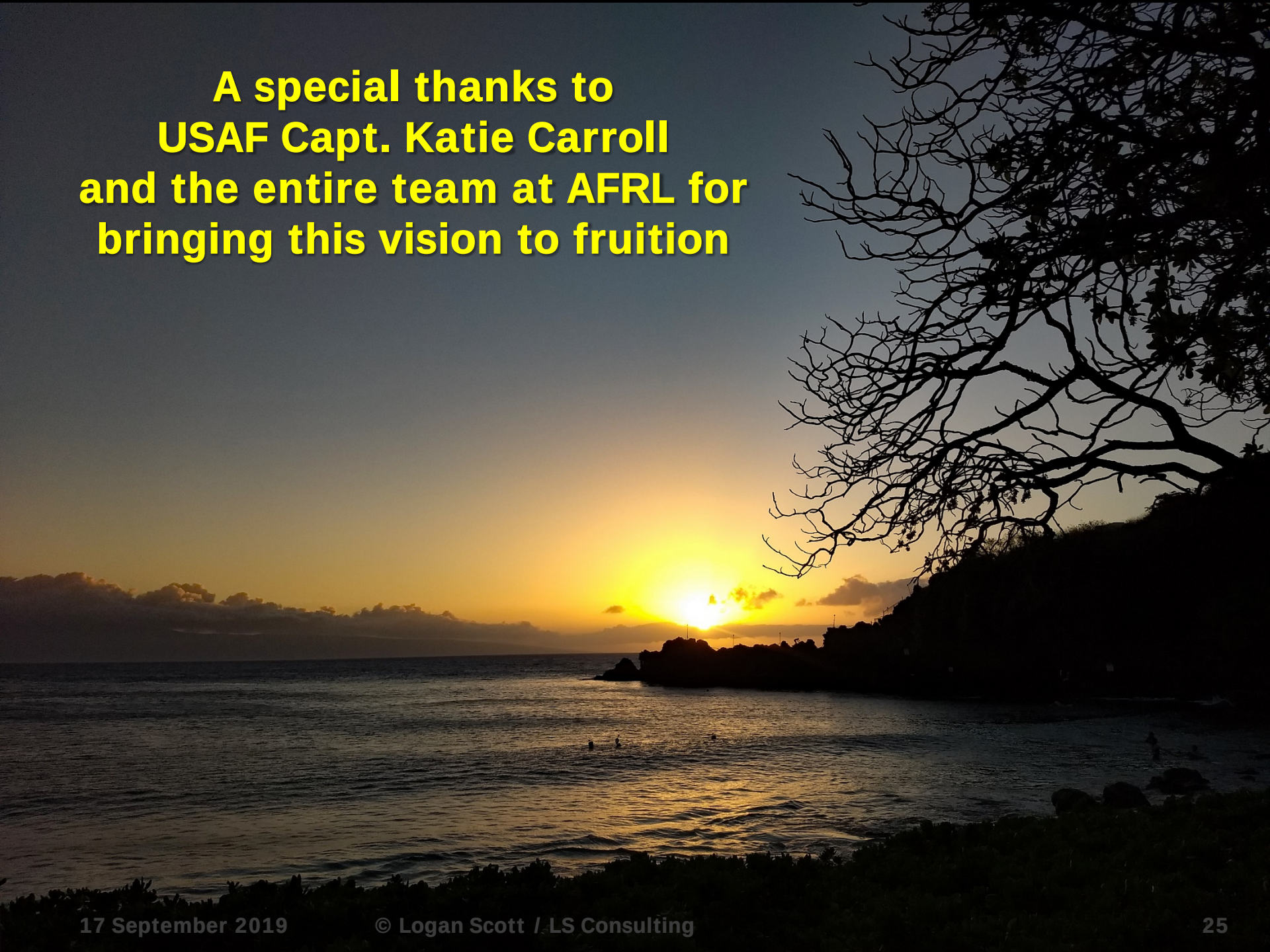
- Who Am I?
  - Username: admin
- What Do I Know?
  - Password: password
- What Do I Have?
  - Token: cell phone authentication app *(NOT SMS!)*
- Where Am I?
  - Location: I'm at the coffeeshop

Prospects for Chimera in US Systems

- Almost ANY navigation signal can be watermarked with backwards compatibility
- Implementing CHIMERA is Not That Hard
  - Message Signing Can Be Done in Software
  - Watermarks are a PN Code Generator Modification in the SV
    - Digital / FPGA Change Only (~6 weeks to modify Block III flight payload)
    - NO Analog or Modulator Changes
- NTS-3 Will Broadcast Chimera on an Experimental Basis
  - 2022 Launch
- Secure-WAAS Signal Design Described in 2003 Paper Remains Valid with a couple of tweaks
  - Modulators are on the Ground
  - Side Channel Approach Requires 5% Power Rise (0.22 dB)

Spoofing Detection Is Becoming More Important: For an AI, Perception is Reality

From "sweet girl" to "racist, hate filled" chatbot in 10 hours


A special thanks to
USAF Capt. Katie Carroll
and the entire team at AFRL for
bringing this vision to fruition


World's Biggest Data Breaches & Hacks
Select losses greater than 30,000 records
https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
Last updated: 1 April 2019
interesting story
Filter
Colour
YEAR
DATA SENSITIVITY
2009
2019
Search...
Latest
2019
2018
2017
2016
Armor Games
BreedReady
DataCamp
EyeEm
Ge.tt
Houzz
8fit
BookMate
Dubsmash 162,000,000
HauteLook
Petflow
Roll20
Vårdguiden
YouNow
Blank Media Games
Chtrbox 49,000,000
Newegg
ShareThis
Stronghold Kingdoms
Toyota
500px
Artsy
Vision Direct
Whitepages
WiFi Finder
Animoto
Blur
Coinmama
Grindr
IBM Company
Orbitz
Ticketmaster
Urban Massage
TicketFly
Firebase
MyHeritage
WordPress
Careem
CMS
Amazon
Cathay Pacific Airways
Dell
Marriott Hotels 383,000,000
Quora 100,000,000
Twitter 330,000,000
ViewFines
Chinese resume leak 202,000,000
Facebook 50,000,000
Google+
Nametests 120,000,000
NMBS
Texas voter records
British Airways
High Tail Hall
Facebook
Zomato
Cellebrite
DaFont
Imgur
Instagram
MyFitnessPal 150,000,000
SKY Brasil
SVR Tracking
TIO Networks
Viacom
Wonga
Bell
CEX
Disqus
Equifax 143,000,000
RootsWeb
Snapchat
Swedish Transport Agency
Uber 57,000,000
Waterly
Yahoo
Malaysian telcos & MVNOs
KM.ru & Nival
Linux Ubuntu forums
Mossack Fonseca
Dailymotion
Weebly
Banner Health
Clinton campaign
Brazzers
ClixSense
Fling
LinkedIn 117,000,000
Mutuelle Generale de la Police
PayAsUGym
Philippines' Commission on Elections
Quest Diagnostics
Syrian government
Three
Turkish citizenship database
Telegram
Dropbox 68,700,000
Interpark
Minecraft
MySpace 164,000,000
Red Cross Blood Service
Tumblr
VK 100,000,000
World Check
Lynda.com
Mail.ru
uTorrent
It's a Good Thing That Our Computer Systems are So Secure