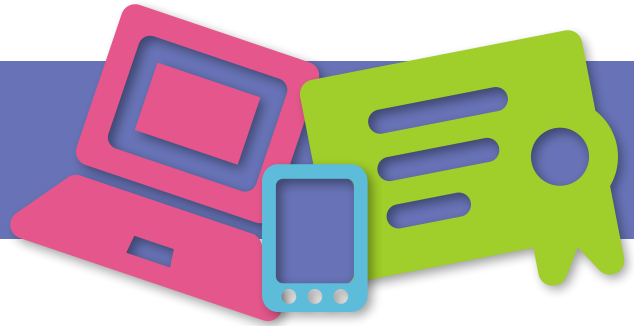
SECURITY 2016
24. ročník konference o bezpečnosti v ICT



Software-Defined Radios Expose NFC and GPS Vulnerabilities

Tomáš Rosa
RaiffeisenBANK

Software-Defined Radio

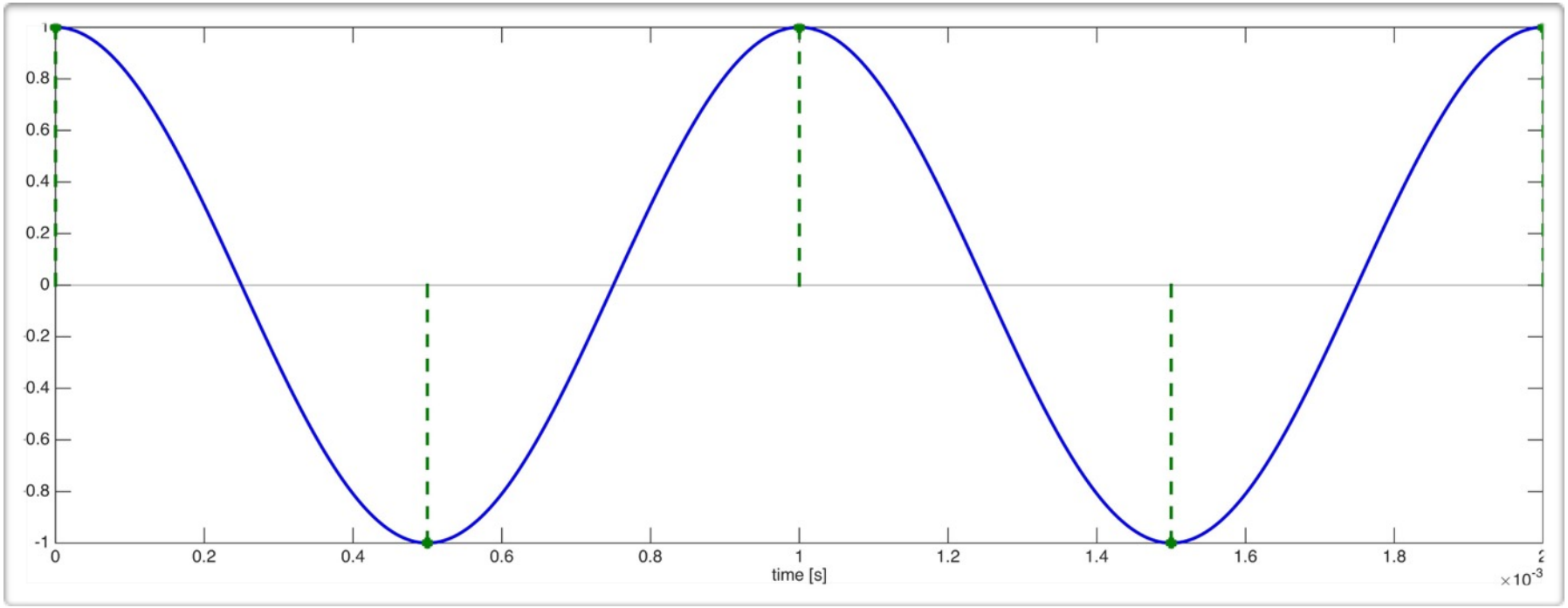
Baseband Sampling Theorem

- *Let s(t) be a Fourier-integrable signal having its highest non–negligible frequency $|f_{max}| < f_s/2 = 1/2T_s$.*
- *Such s(t) can be then fully reconstructed from its discrete-time samples as:*

$$s(t) = \sum_{k=-\infty}^{\infty} s(kT_s) \frac{\sin \pi(\frac{t - kT_s}{T_s})}{\pi(\frac{t - kT_s}{T_s})} = \sum_{k=-\infty}^{\infty} s(kT_s) \operatorname{sinc}(\frac{t - kT_s}{T_s})$$

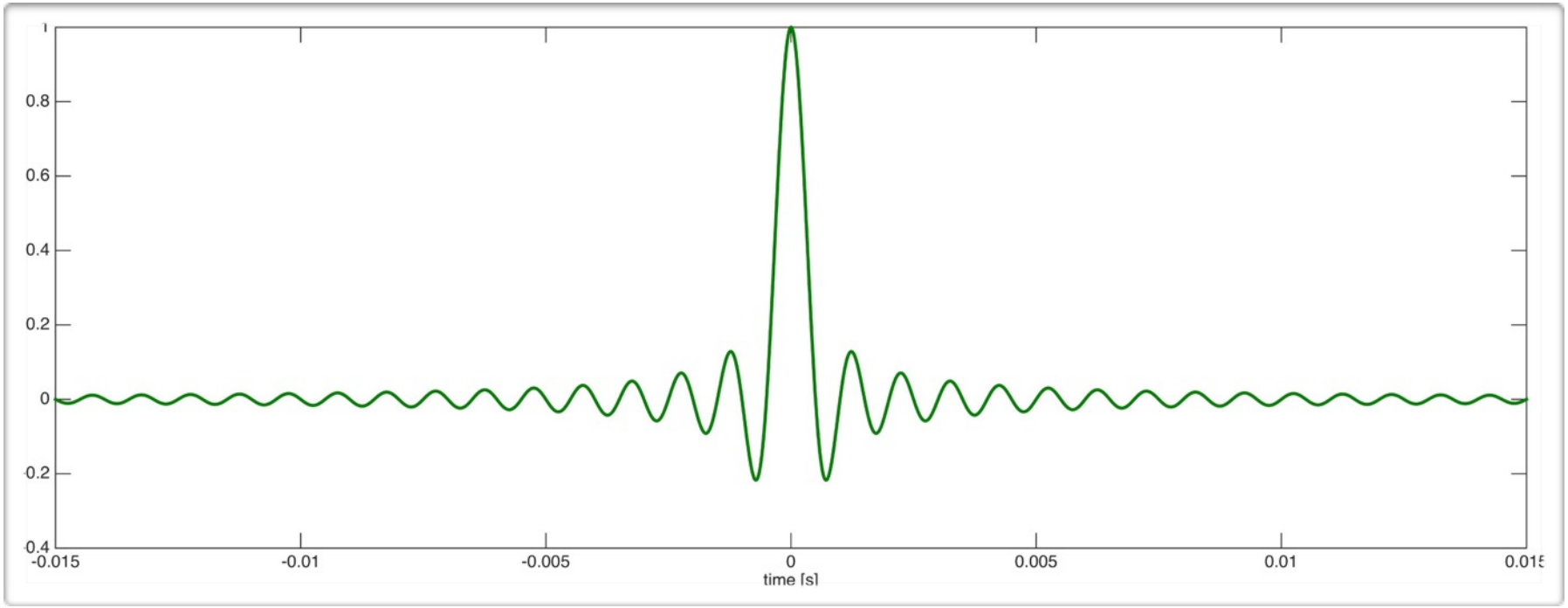
— Kotelnikov, Nyquist, Shannon, Whittaker

Limit Example - Nyquist Rate Sampling of Even Harmonics



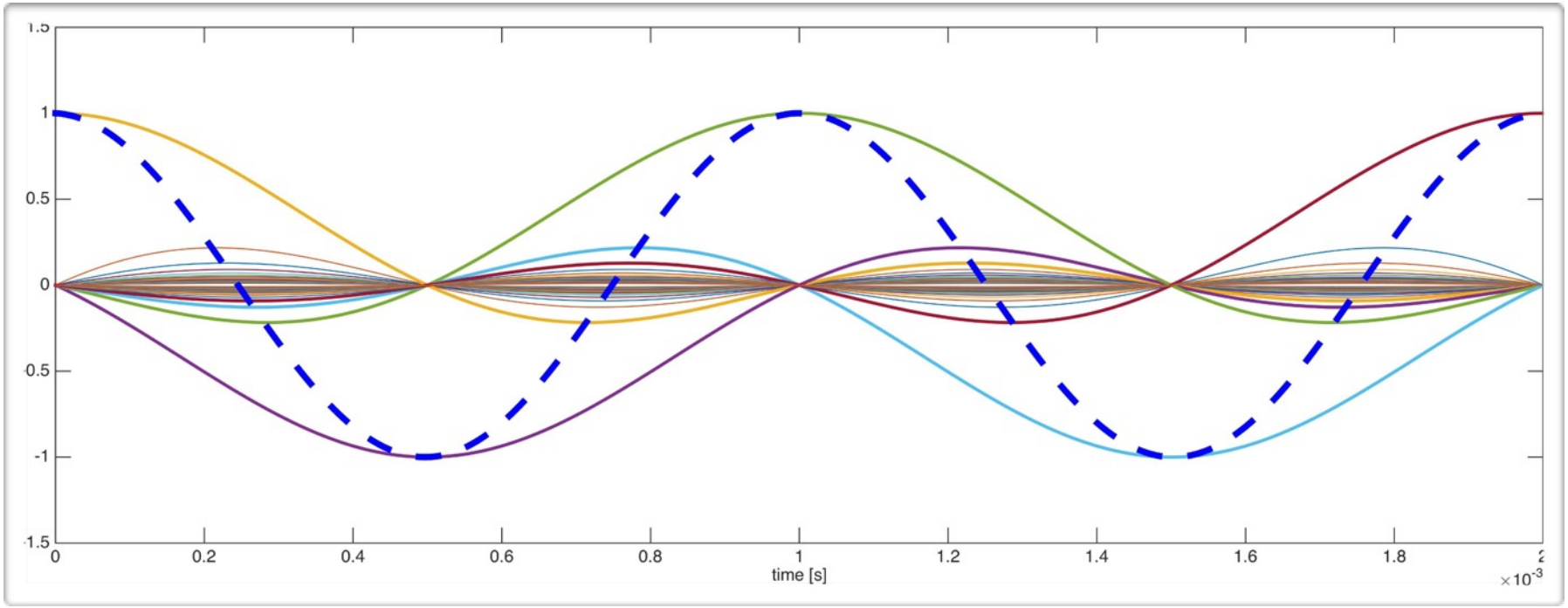
1 kHz @ Nyquist sample rate f_s = 2 kHz

Sinus Cardinalis



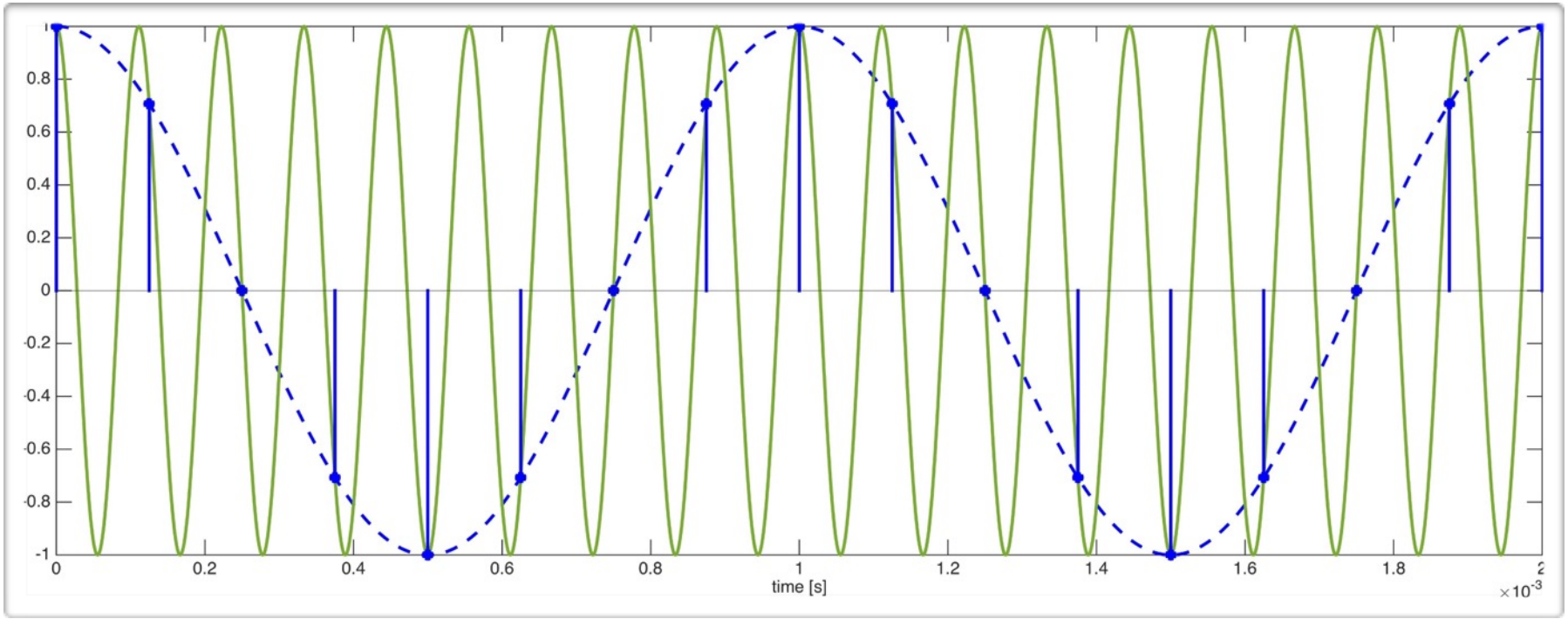
in lowpass filter impulse response scale @ 1 kHz

Interpolation



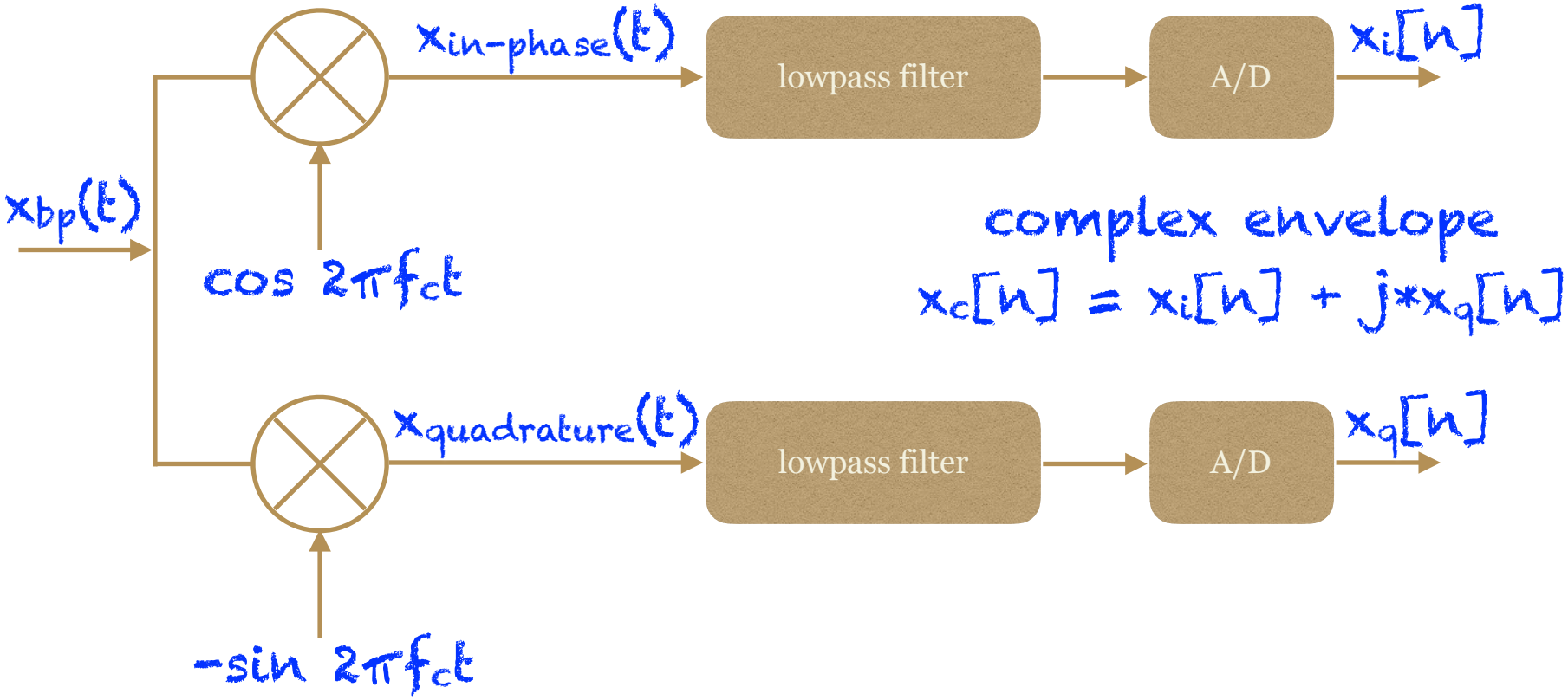
1 kHz recovered @ f_s = 2 kHz with 30-sample delay

Aliasing Example



9 kHz -> 1 kHz @ sample rate f_s = 8 kHz

Bandpass Signal Quadrature Sampling



complex envelope

$x_c[n] = x_i[n] + j*x_q[n]$

bandpass complex signal sampling at $f_s = B$

cf. [Lyons, 2011] for an excellent explanation

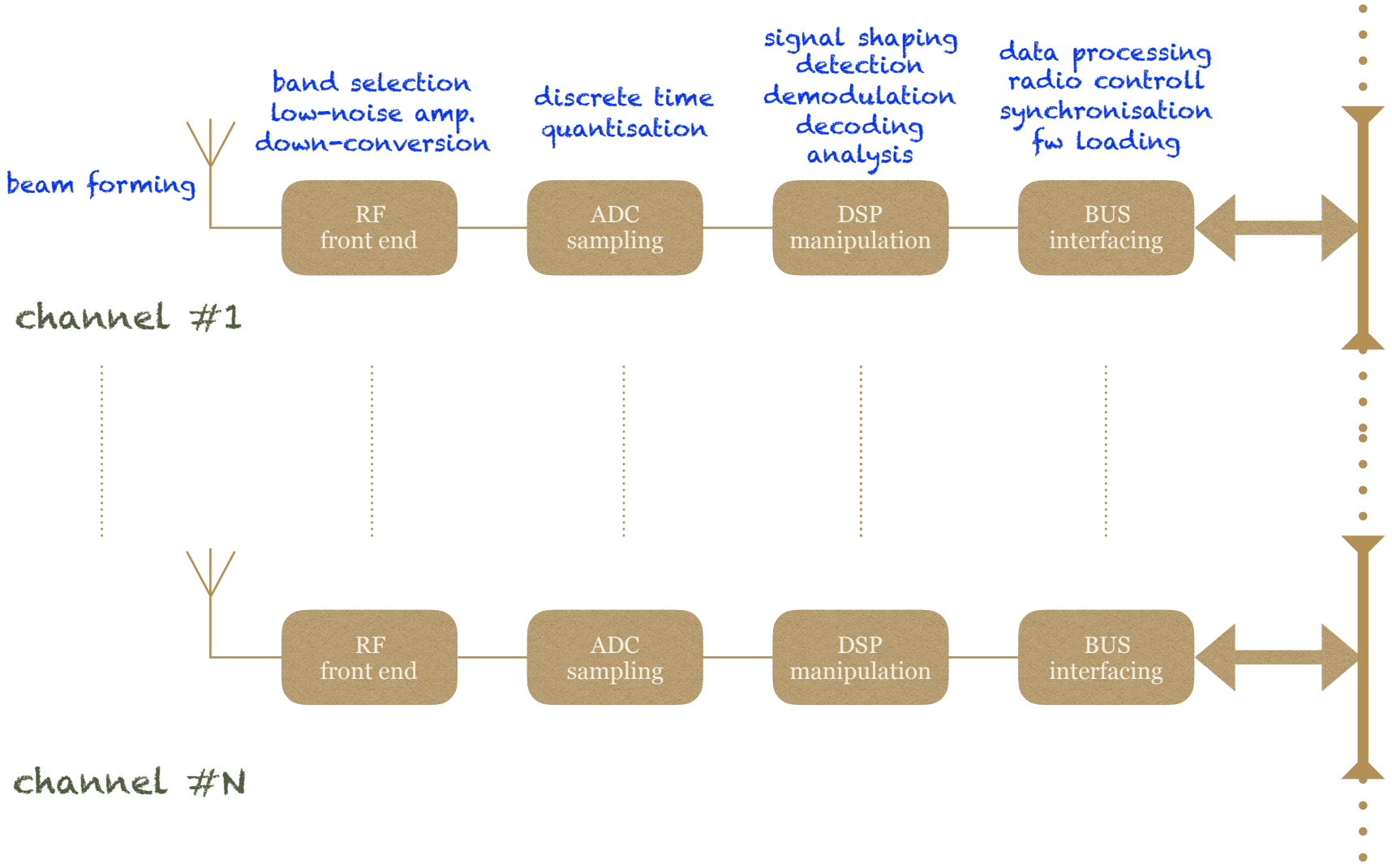
Digital Signal Processing (DSP)

… uses the correspondence of continuous-time functions and discrete-time sequences to process the input signals by digital operations instead of analog circuits

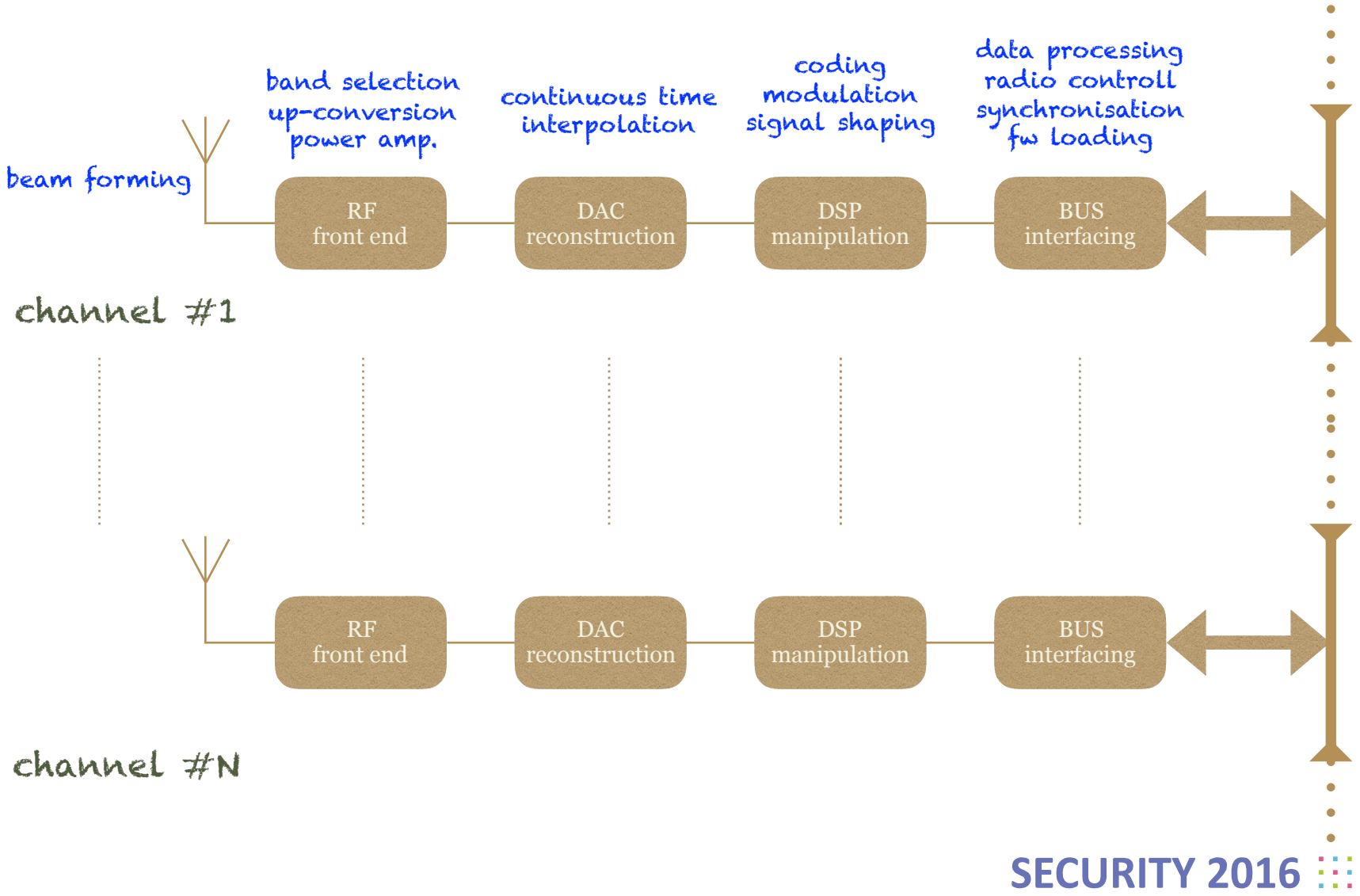
Software-Defined Radio (SDR)

… components that have been typically implemented in (analog) hardware are instead implemented by means of software on a personal computer or an embedded system

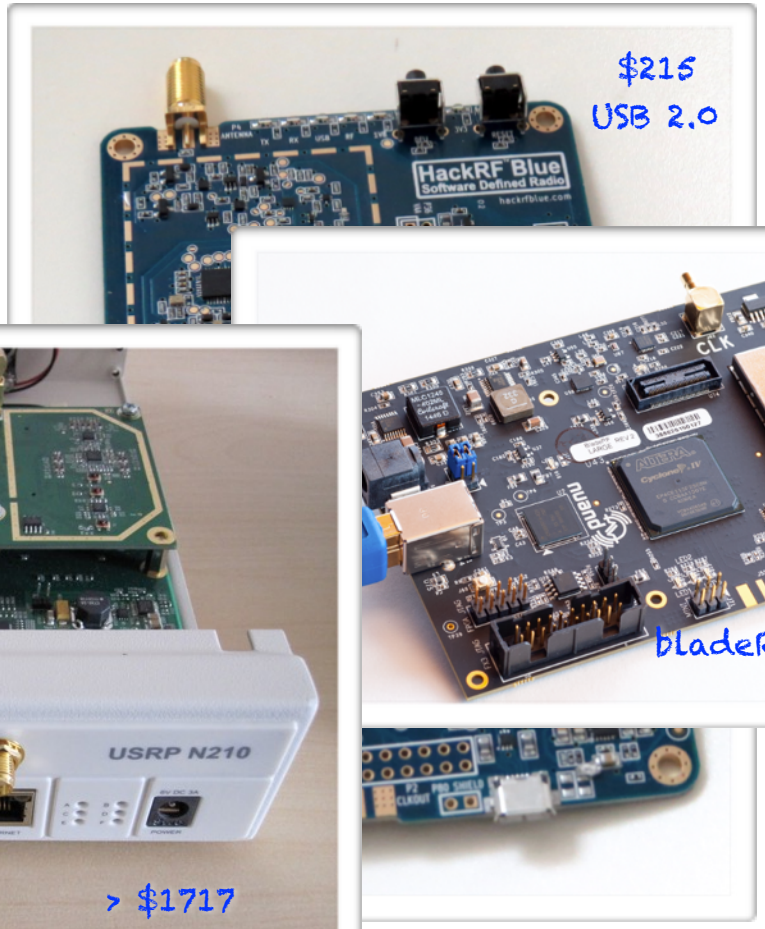
SDR Concept - RX Path



SDR Concept - TX Path



Popular Hacking SDRs



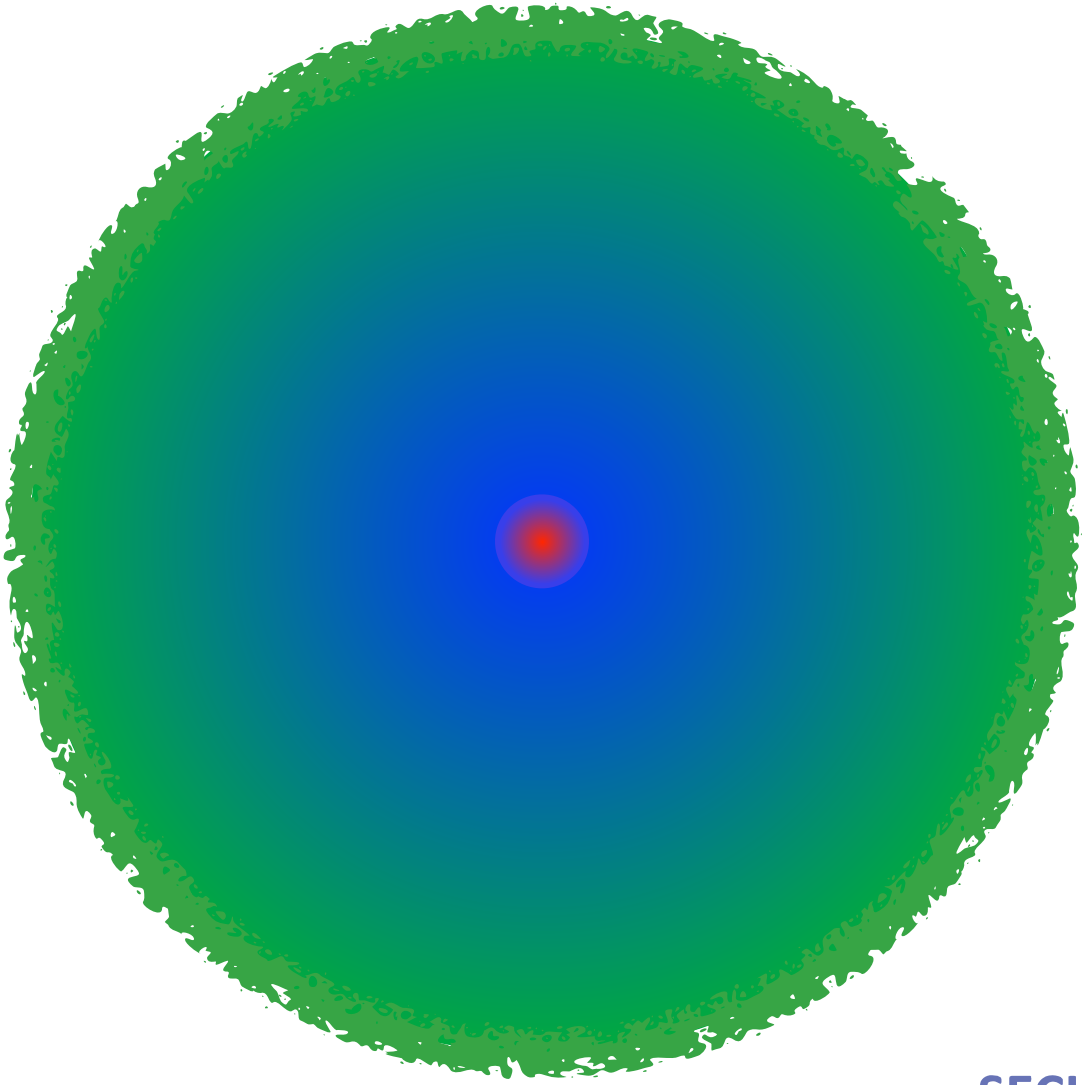
SDR As a Threat

DSP routines are SW. This can be shared, installed, and executed all around the world instantly with a very modest background.

Just like any other exploit code.

Near Field Communication

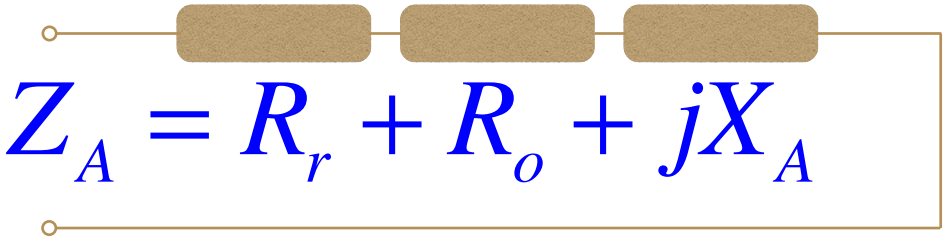
EM Radiation Regions



Near, Far, Wherever You Are…

- Basing on the different dominating EM field components implying different dominating field behaviour, it is useful to distinguish:
  - *Reactive near field* (XNF). Energy is mainly stored and exchanged between *E* and *H*. It is closest to the radiator and evades as $1/r^3$.
  - *Radiating near field* (Fresnel region). Energy is mainly radiated with unstable patterns, however. It starts roughly with $r > \lambda/2\pi$ and evades continuously with $1/r^2$.
  - *Far field* (Fraunhofer region). Energy is radiated with a distance-independent field pattern. Several conditions shall be met: $r > 2D^2/\lambda$, $r > 5D$, $r > 1.6\lambda$, where *D* is the largest antenna dimension. It evades continuously with $1/r$.

Antenna Impedance



- The input impedance Z_A describes the antenna from the lumped circuit parameters viewpoint. *It also encapsulates the observable antenna field behaviour.*
  - R_r is the equivalent radiation resistance representing the energy emanated through the radio waves
  - R_o describes the dissipative energy loss
  - X_A reflects the energy exchanged back-and-forth with the reactive near field

Yes, It Can!

- NFC antenna is generally capable of transmitting its signal into the far field region
- Due to its construction, the radiation resistance is very small leading to a very poor energy transfer
- Nevertheless, it does not mean there is no transmission at all

Parasitic Antennas

- From the security viewpoint, we shall recognise it may not be the *primary* antenna only that can radiate sensitive data
- In general, any spatial distribution of a time-varying current modulated (or sensed!) by the internal processing unit is a potential backdoor
  - we are getting to the well-known phenomenon of the electromagnetic side-channels
  - in principle, applying anti-RFI techniques for all those patch cables and power lines is a good idea to start with

Initiator Range Extension

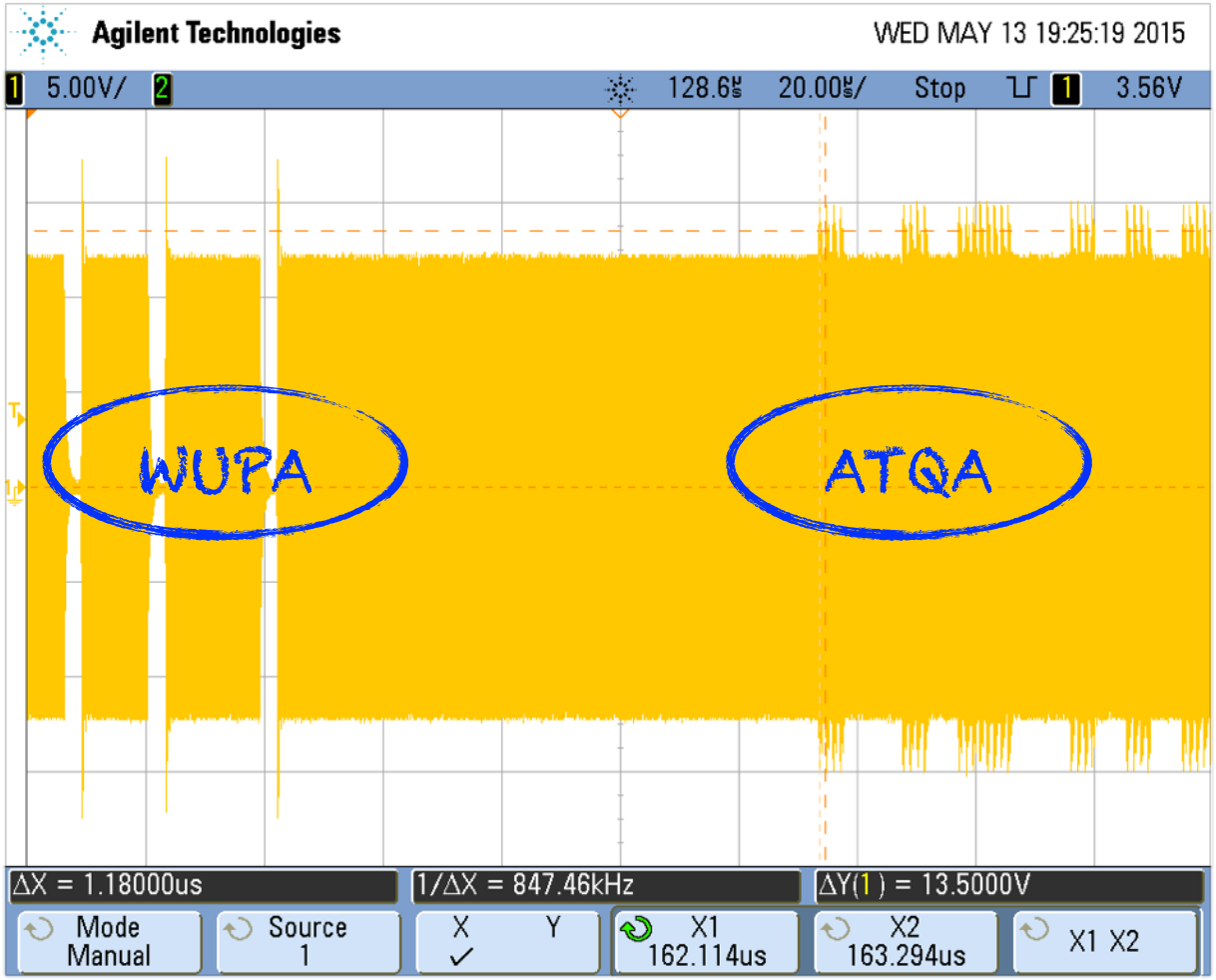
- Allows RF skimming or wormhole (relay) attacks
- Due to a very low efficiency and very high power consumption, it is practically limited to the reactive near field region (XNF)
- Antenna diversity separating downlink and uplink channels may help significantly
- Distance: Decimetres (confirmed), reliably working at around 20 cm. Principal upper limit ≈ $\lambda/2\pi$, i.e. circa 3.5 m, is infeasible to achieve practically. So, we are limited to a kind of *bumping attack*.

Sniffing

- Sensitive data capture, identity theft
- **Often, this scenario induces the most serious risks**
- Works over all zones, from XNF to Fraunhofer region
- For regions outside XNF, the important idea is to look for higher harmonics of the 13.56 MHz carrier
- Distance: Metres to dekametres. Confirmed for both downlink and uplink channels.

All You Need is *Loop*

Intercepted Signal Example (NFC-A)



Spying in the Lane (Still in XNF)

[https://www.youtube.com/watch?v=9QjxwejBPHs]

Going Far → Small Loop (HAM Illustration)

[AlexLoop by Gary, KE2YK]

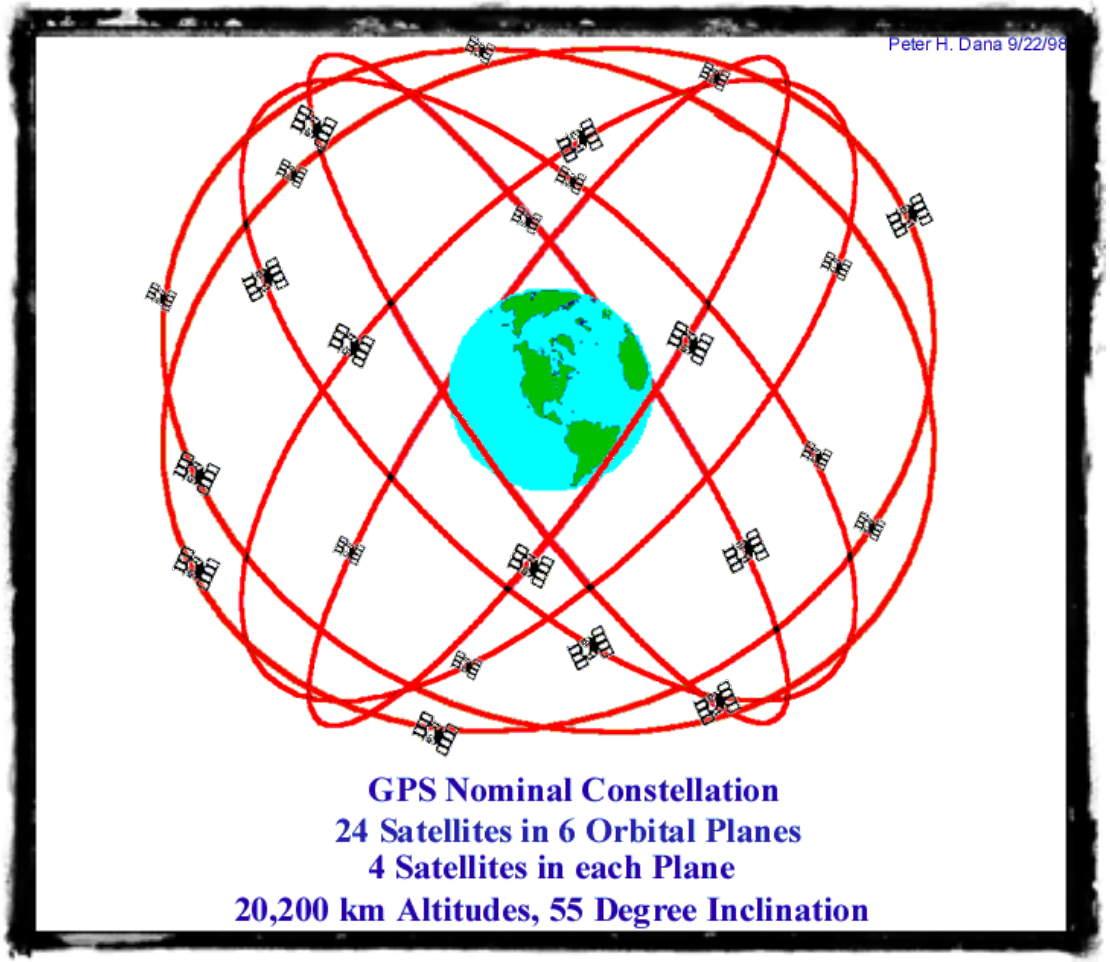
The Show Still Goes On…

- ✓ Target range extension (metres, confirmed)
- ✓ Traffic injection - MITM (decimetres to metres for uplink TX only, confirmed)
- ✓ Initiator location (dekametres, confirmed)
- ✓ Target location (decimetres confirmed to metres estimated)
- ✓ Jamming (metres confirmed to dekametres estimated)
- ✓ Device destruction (decimetres)

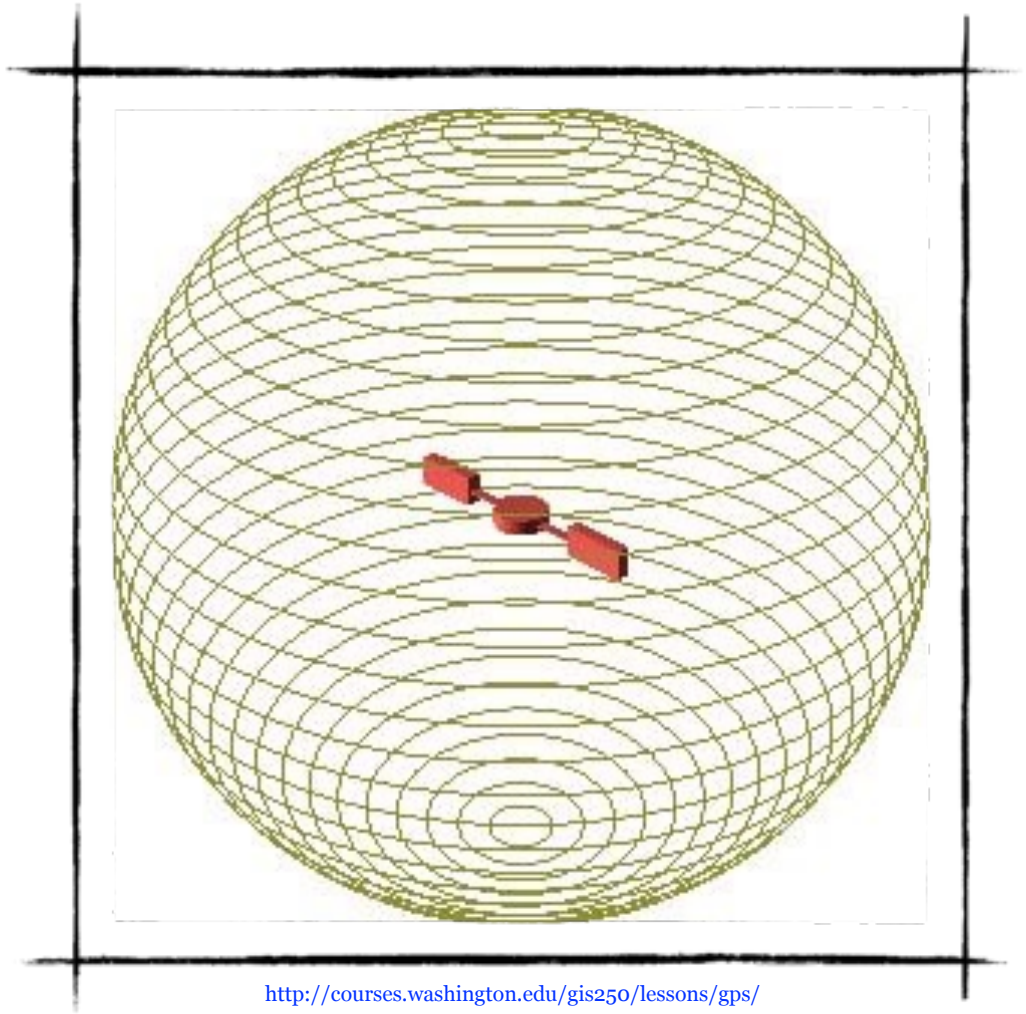
NAVSTAR
Global Positioning System

Space Segment Vehicle (Block IIF)

GPS Space Segment

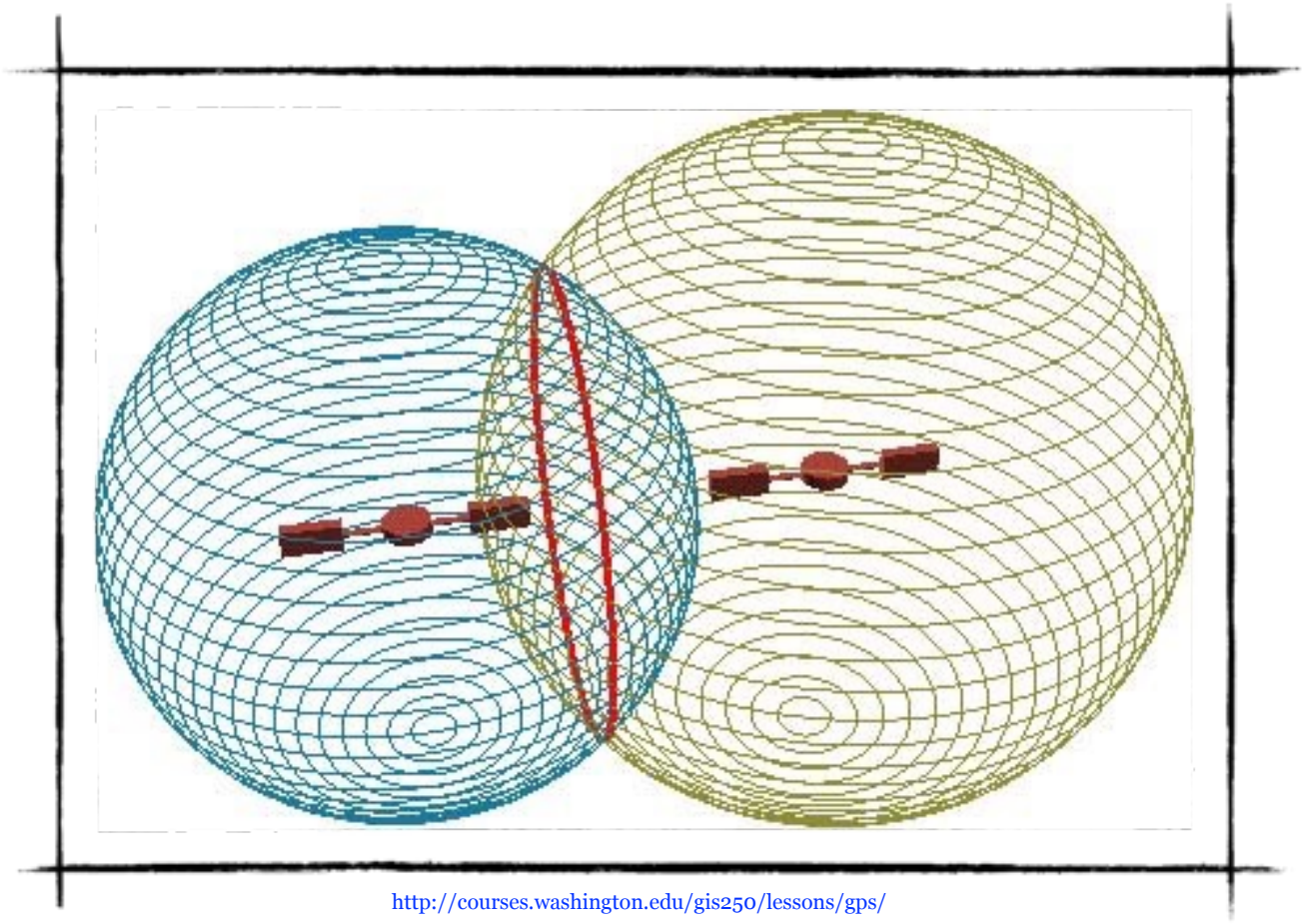


Trilateration I



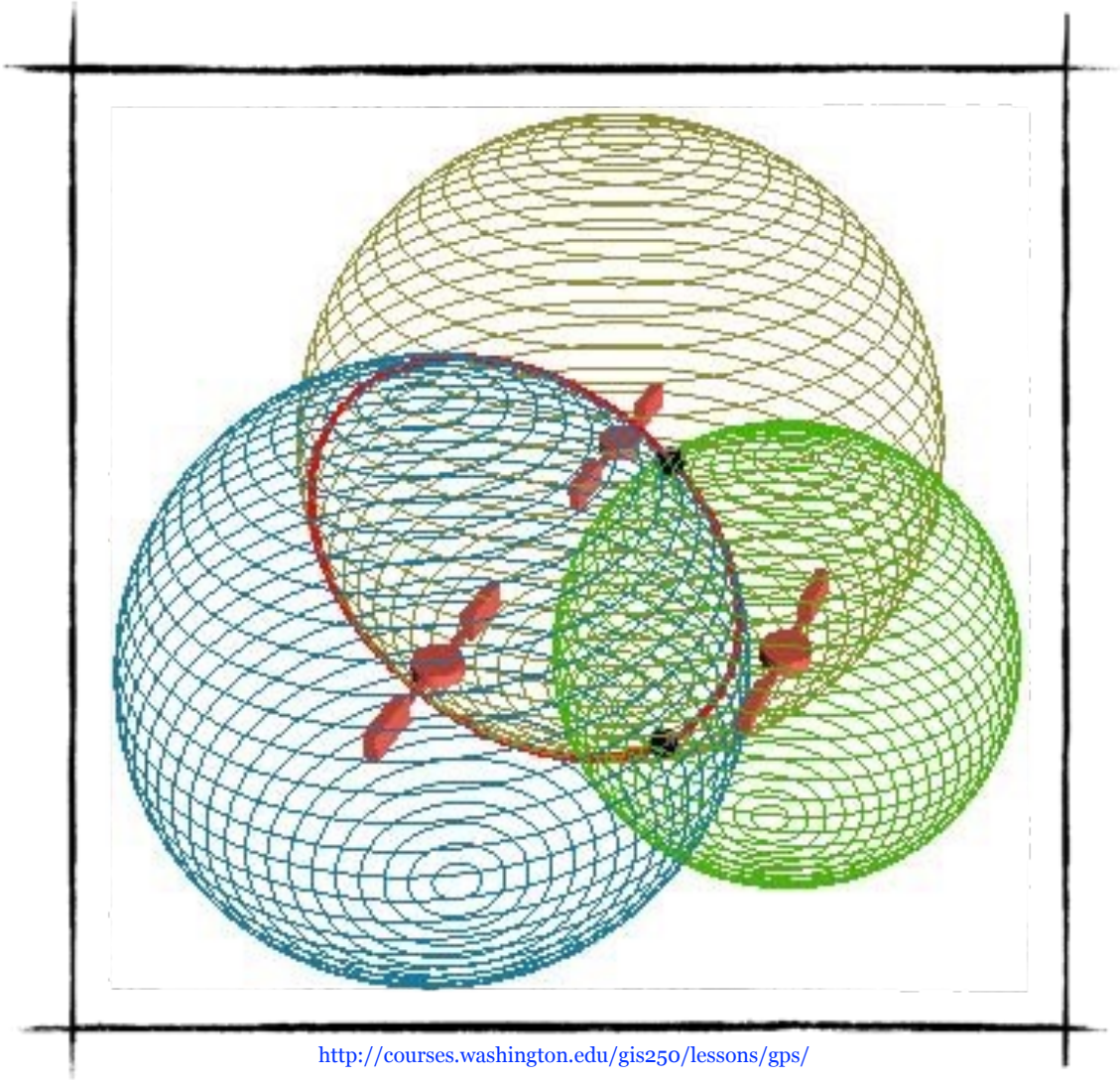
http://courses.washington.edu/gis250/lessons/gps/

Trilateration II



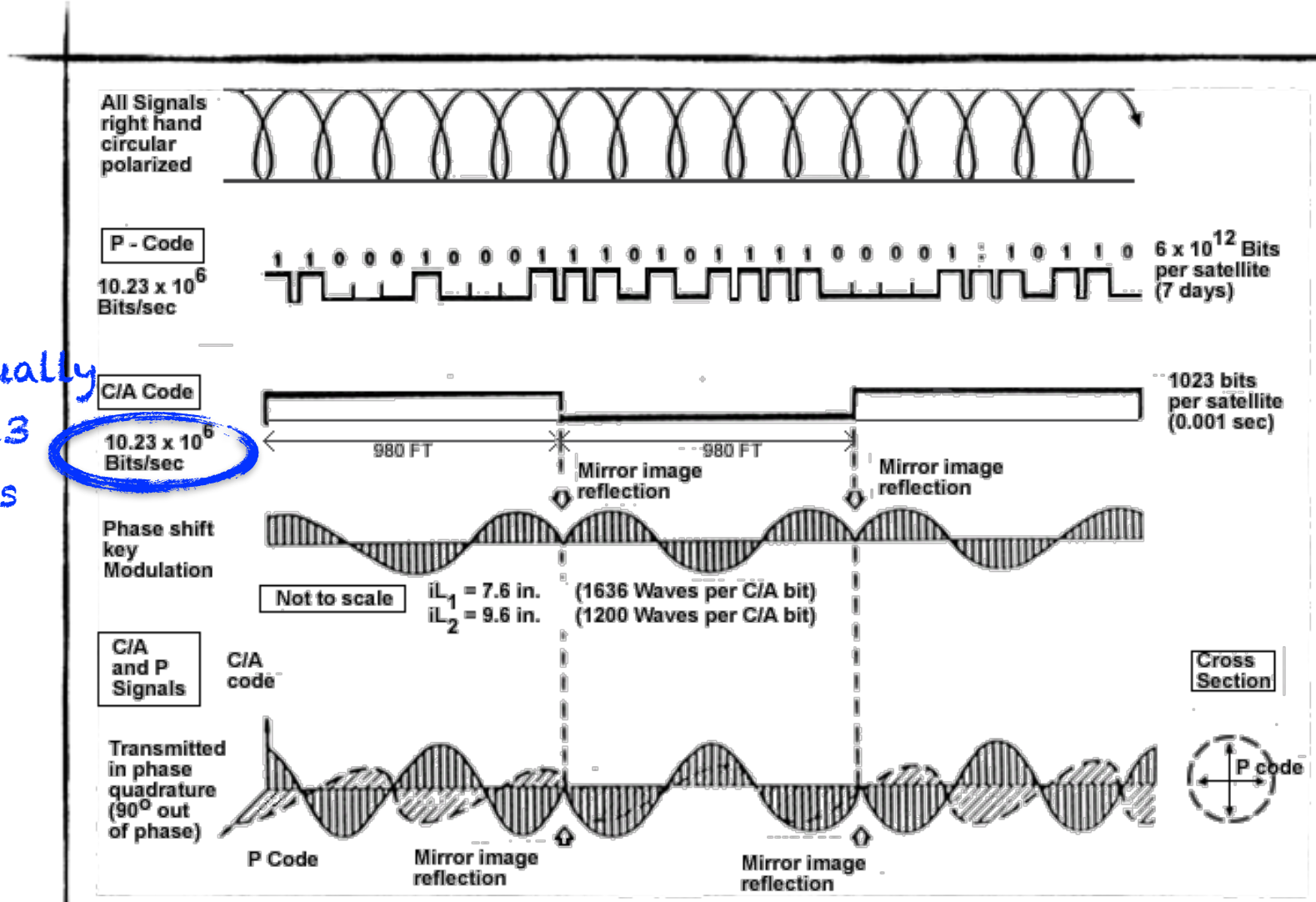
http://courses.washington.edu/gis250/lessons/gps/

Trilateration III



http://courses.washington.edu/gis250/lessons/gps/

GPS L1 C/A ⊗ P(Y) (Illustration ONLY)



actually 1.023 Mbps

Kulshreshta, 1997

Satellite Clock Replicas Expose Time Delays

t_{sent_sv1}

t_{sent_sv2}

t_{sent_sv3}

four SVs to get
X, Y, Z, and t_{bias}

t_{sent_sv4}

$t_{rec}+t_{bias}$

Civil GPS in Serious Applications

NTP server

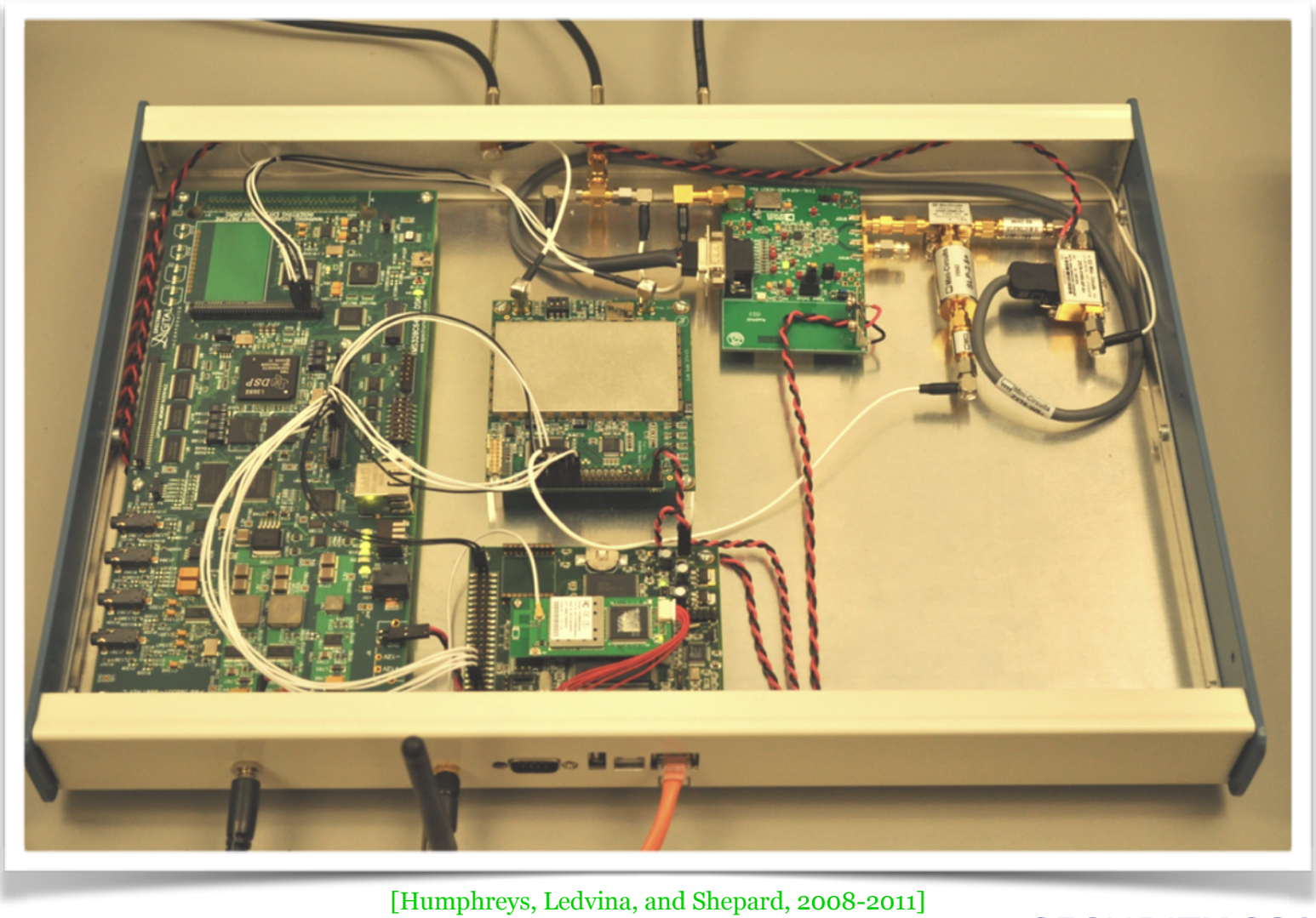
L1 C/A Signal in Brief

- CDMA at the common carrier frequency of 1575.42 MHz
  - BPSK-R(1) Direct Sequence Spread Spectrum (DSSS) according to the notation of [Betz, 2016]
- Satellites distinguished by their unique chipping sequence (Gold codes)
- Allows creation of a delayed replica clock of the particular satellite (implicit time synchronisation)
- Carries 37 500 bits of navigation data for the particular satellite (explicit time synchronisation and position computation)
- Includes corrections according to the General Theory of Relativity
- … does not include any cryptographic protection

L1 C/A Security

- Position/Velocity/Time (PVT) spoofing is accessible to a moderate-level attacker
  - real-life scenario may (allegedly) be that **“Iran-U.S. RQ-170 incident”**
  - actually, a GPS “replay attack” is a standard advanced tutorial for the LabView platform using the USRP Software Defined Radio (SDR)
- OK, this signal was never meant as a military-grade service and the lack of protection here can hardly be called a “discovery”
- On the other hand, a lot of L1 C/A applications have grown up to be vital parts of our critical infrastructure today…

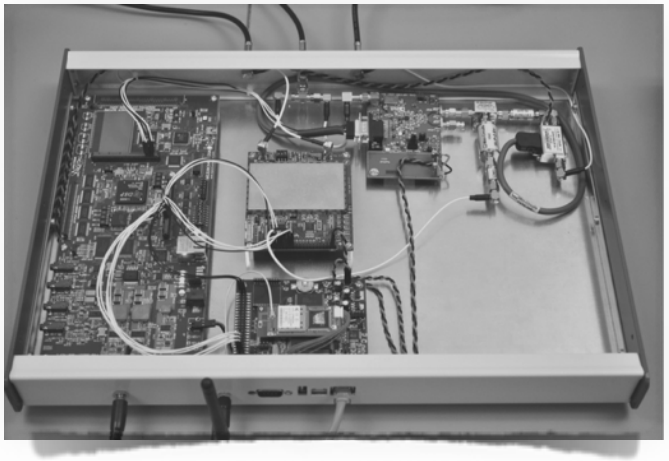
Civil GPS Under Serious Attack



[Humphreys, Ledvina, and Shepard, 2008-2011]

Precise SDR Spoofer

- receiver-spoofer (MITM) architecture
- tracks original L1 C/A and L2C
- manipulates individual SV signal channels of L1 C/A (up to 12)
- re-mixes and re-transmits the spoofed signal
- precise phase sync for a smooth take over
- SDR architecture; someday it could be just downloaded and run
- HW parts were off-the-shelf components of approx. $1500 (2008)



[Humphreys, Ledvina, and Shepard, 2008-2011]

Achievements Announced in Public

[Bhatti, Humphreys, Ledvina, Pesyna, Shepard, Huang, Yang, et al. - cf. references]

SBAS to the Rescue?

- Satellite-Based Augmentation System in general
  - European Geostationary Navigation Overlay Service (EGNOS), for example, in particular
- Provides integrity report and differential corrections for the original L1 C/A signal
  - However, it rather applies to the *transmitted signal*, instead of the signal received by the individual user station

In Other Words

"…Degradations of the received signal that occur after transmission, such as … reception of invalid signals transmitted by others, *are not addressed* by SBAS integrity indications."

– [Betz, 2016]

The Next Target?

- Recall those 37 500 bits of navigation data transmitted on each and every L1 C/A channel
- It has been observed the baseband processors in GPS user modules seldom care about the integrity of this data as well as of the plausibility of PVT results obtained
  - [Sheppard and Humphreys, 2011], [Nighswander et al., 2012]
- Interestingly, this suggests a new infection vector allowing malware installation right into the GPS receiver…

Conclusion

- RF signals are ubiquitous, we probably cannot live without all that electromagnetic tweeting anymore
- Often, the relative inaccessibility of the RF interface is the only protection
- SDR phenomenon offers an unprecedentedly easy access to the whole RF spectrum, while also allowing the rapid and massive exploit sharing
- The era of intensive RF hacking is coming and it will go far beyond the usual scope of Wi-Fi and Bluetooth!


REALLY, DO THE PENTEST!

References - Common

1. Balanis, C.-A.: *Antenna Theory - Analysis and Design*, Third Edition, Wiley-Interscience, 2005
2. Boggess, A. and Narcowich, F.-J.: *A First Course in Wavelets with Fourier Analysis*, Second Edition, Wiley, 2009
3. Essick, J.: *Hands-On Introduction to LabVIEW for Scientists and Engineers*, Third Edition, Oxford University Press, 2015
4. Grayver, E.: *Implementing Software Defined Radio*, Springer, 2012
5. Griffiths, D.-J.: *Introduction to Electrodynamics*, Fourth Edition, Pearson, 2013
6. James, J.-F.: *A Student's Guide to Fourier Transforms With Applications in Physics and Engineering*, Third Edition, Cambridge University Press, 2011
7. Johnson, C.-R., Jr., Sethares, W.-A., and Klein, A.-G.: *Software Receiver Design - Build Your Own Digital Communications System in Five Easy Steps*, Cambridge University Press, 2011
8. Kraus, J.-D. and Fleish, D.-A.: *Electromagnetics with Applications*, Fifth Edition, McGraw-Hill, 1999
9. Kraus, J.-D. and Marhefka, R.-J.: *Antennas For All Applications*, Third Edition, McGraw-Hill, 2003
10. Lathi, B.-P. and Green, R.-A.: *Essentials of Digital Signal Processing*, Cambridge University Press, 2014
11. Lyons, R.-G.: *Understanding Digital Signal Processing*, Third Edition, Prentice Hall, 2011
12. Pu, D. and Wyglinski, A.-M.: *Digital Communication Systems Engineering with Software-Defined Radio*, Artech House, 2013
13. Stutzman, W.-L. and Thiele, G.-A.: *Antenna Theory and Design*, Third Edition, Wiley, 2013

References - NFC

14. Brown, T.-C.-W. and Diakos, T.: *On the Design of NFC Antennas for Contactless Payment Applications*, 2011

15. Brown, T.-C.-W., Diakos, T., and Briffa, J.-A.: *Evaluating the Eavesdropping Range of Varying Magnetic Field Strengths in NFC Standards*, 2013

16. Diakos, T.-P., Briffa, J.-A., Brown, T.-W.-C., and Wesemeyer, S.: *Eavesdropping near-field contactless payments: a quantitative analysis*, 2013

17. Engelhardt, M., Pfeiffer, F., Finkenzeller, K., and Biebl, E.: *Extending ISO/IEC 14443 Type A Eavesdropping Range using Higher Harmonics*, 2013

18. Finkenzeller, K.: *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*, Third Edition, Wiley, 2010

19. Finkenzeller, K.: *Research Homepage*, http://rfid-handbook.de [checked Nov-23-2015]

20. Finkenzeller, K.: *Known attacks on RFID systems, possible countermeasures and upcoming standardisation activities*, 2009

21. Finkenzeller, K.: *Battery powered tags for ISO/IEC 14443, actively emulating load modulation*, 2011

22. Finkenzeller, K., Pfeiffer, F., and Biebl, E.: *Range Extension of an ISO/IEC 14443 type A RFID System with Actively Emulating Load Modulation*, 2011

23. Francis, L., Hancke, G.-P., Mayes, K., and Markantonakis, K.: *Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones*, 2011

References - NFC

24. Hancke, G.-P.: *Research Homepage*, http://www.rfidblog.org.uk/research.html [checked Nov-23-2015]

25. Hancke, G.-P.: *Practical Eavesdropping and Skimming Attacks on High-Frequency RFID Tokens*, 2011

26. Kfir, Z. and Wool, A.: *Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems*, 2005

27. Kirschenbaum, I. and Wool, A.: *How to Build a Low-Cost, Extended-Range RFID Skimmer*, 2006

28. Lee, Y.: *Antenna Circuit Design for RFID Applications*, Application Note 710, Microchip Tech. Inc., 2003

29. NXP: *AN1445 - Antenna design guide for MFRC52x, PN51x, and PN3x*, 2010

30. Oren, Y., Schirman, D., and Wool, A.: *Range Extension Attacks on Contactless Smart Cards*, 2013

31. Pfeiffer, F., Finkenzeller, K., and Biebl, E.: T*heoretical Limits of ISO/IEC 14443 type A Eavesdropping Attacks*, 2012

32. Rosa, T.: *RFID Wormholes – the Case of Contactless Smart Cards*, 2011

33. Thevenon, P.-H., Savry, O., Tedjini, S., and Malherbi-Martins, R.: *Attacks on the HF Physical Layer of Contactless and RFID Systems*, 2011

References - NFC

34. ISO/IEC 14443-1: *Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 1: Physical characteristics*, 2000

35. ISO/IEC 14443-2: *Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 2: Radio frequency power and signal interface*, 2001

36. ISO/IEC 14443-3: *Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 3: Initialization and anticollision*, 2001

37. ISO/IEC 14443-4: *Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 4: Transmission protocol*, 2001

38. ISO/IEC 18092: *Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1)*, 2004

39. NFC Forum: *NFC Digital Protocol*, Technical Specification, 2010

40. EMV Contactless Specifications for Payment Systems: *Book D - EMV Contactless Communication Protocol Specification*, 2015

References - GPS / GNSS

41. Betz, J.-W.: *Engineering Satellite-Based Navigation and Timing: Global Navigation Satellite Systems, Signals, and Receivers*, IEEE Press, John Wiley & Sons, 2016

42. Bonebrake C. and O'Neil, L.-R.: *Attacks on GPS Time Reliability*, IEEE Security & Privacy, May/June 2014, pp. 82-84, 2014

43. Borre, K., Akos, D.-M., Bertelsen, N., Rinder, P., Jensen, S.-H.: *A Software-Defined GPS and Galileo Receiver (Applied and Numerical Harmonic Analysis)*, Birkhäuser Boston, 2007

44. Chen, J., Zhang, S., Wang, H., and Zhang, X.: *Practicing a record-and-replay system on USRP*, In Proc. of the second workshop on Software radio implementation forum, pp. 61-64. ACM, 2013

45. Doberstein, D.: *Fundamentals of GPS Receivers - A Hardware Approach*, Springer, 2011

46. Fernández-Prades, C., Arribas, J., and Closas, P.: *Turning a television into a GNSS receiver*, In Proc. of ION GNSS, pp. 1492-1507. 2013

47. Huang, L. and Yang, Q.: *GPS Spoofing - Low-cost GPS Simulator*, DEF CON 23, Las Vegas, August 6th - 9th, 2015

48. Humphreys, T.-E., Ledvina, B.-M., Psiaki, M.-L., O'Hanlon, W.-O., and Kintner, P.-M., Jr.: *Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer*, In Proc. of the ION GNSS international technical meeting of the satellite division, vol. 55, p. 56. 2008

49. Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., Lachapelle, G.: *GPS vulnerability to spoofing threats and a review of antispoofing techniques*, International Journal of Navigation and Observation, 2012

50. Kaplan, E.-D. and Hegarty, C.-J. (Eds): *Understanding GPS - Principles and Applications*, Second Edition, Artech House, 2006

51. Malhotra, A,, Cohen, I.-E., Brakke, E., Goldberg, S.: *Attacking the Network Time Protocol*, First public posting manuscript, October 21, 2015

References - GPS / GNSS

52. McMilin, E.-B., Chen, Y.-H., De Lorenzo, D.-S., Akos, D.-M., Walter, T.-F., Lee, T.-H., Enge, P.-K.: *Single Antenna, Dual Use: Theory and Field Trial Results for Aerial Applications of Anti-Jam and Spoof Detection*, Inside GNSS, September/October 2015, pp. 40-53, 2015

53. Misra, P. and Enge, P.: *Global Positioning System - Signals, Measurements, and Performance*, Revised Second Edition, Ganga-Jamuna Press, 2012

54. Nighswander, T., Ledvina, B., Diamond, J., Brumley, R., and Brumley, D.: *GPS Software Attacks*, In Proc. of the 2012 ACM conference on Computer and communications security, pp. 450-461, ACM, 2012

55. Shepard, D.-P. and Humphreys, T.-E.: *Characterization of Receiver Response to Spoofing Attack*, In Proc. of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation, p. 2608, 2011

56. Shepard, D.-P., Humphreys, T.-E., and Fansler, A.-A.: *Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks*, International Journal of Critical Infrastructure Protection 5, no. 3, pp. 146-153, 2012

57. Thompson, E.-A., Clem, N., Renninger, I., and Loos, T.: *Software-defined GPS receiver on USRP-platform*, Journal of Network and Computer Applications 35, no. 4 pp. 1352-1360, 2012

58. Tippenhauer, N.-O., Pöpper, C., Rasmussen, K.-B., and Capkun, S.: *On the requirements for successful GPS spoofing attacks, In Proc. of the 18th ACM conference on Computer and communications security*, pp. 75-86. ACM, 2011

59. John A. Volpe National Transportation Systems Center: V*ulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System*, Final Report for the Office of the Assistant Secretary for Transportation Policy, U.S. Department of Transportation, August 29, 2001

60. Wan, X. and Zhan, X.: *The research of indoor navigation system using pseudolites*, Procedia Engineering 15 (2011), pp. 1446-1450, 2011

SECURITY 2016

24. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Tomáš Rosa, Ph.D., OK1SFU
RaiffeisenBANK
tomas.”my_last_name”@rb.cz