



THE UNIVERSITY OF TEXAS AT AUSTIN  
**RADIONAVIGATION LABORATORY**

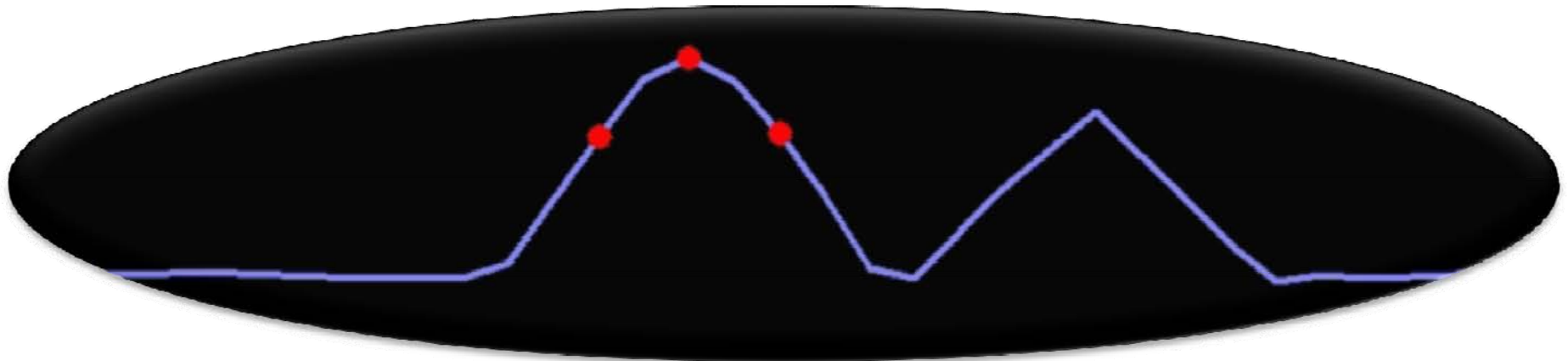
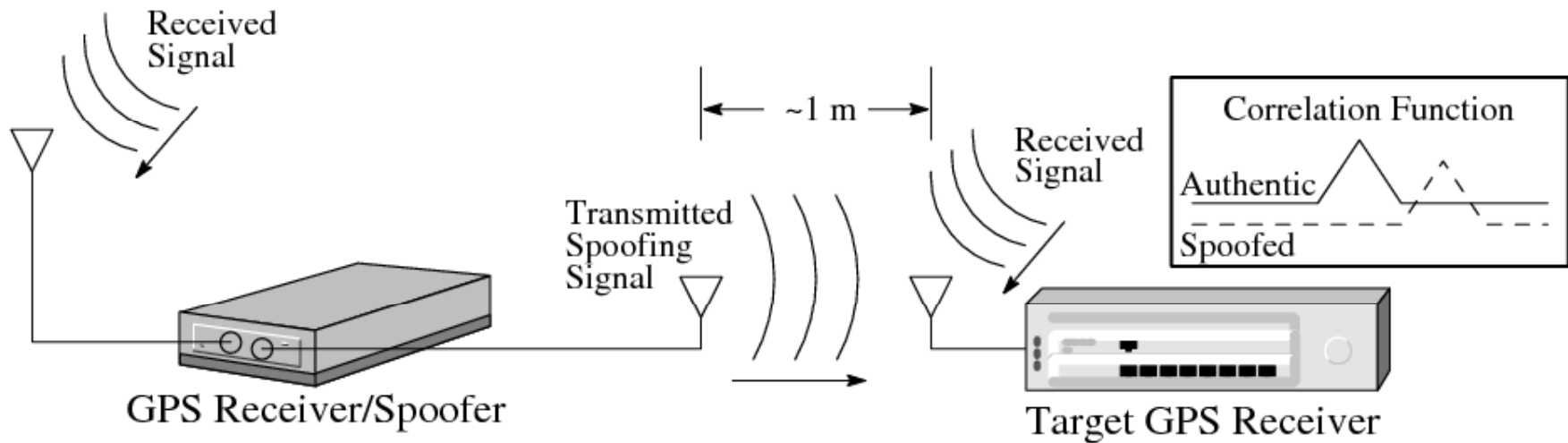


# Spooing Civil GPS-Based Timing

Todd Humphreys

The University of Texas at Austin

# Emerging Threat: Civil GPS Spoofing



---

# Spoofing and Jamming are Different Threats

- Spoofing is more difficult & costly
- Spoofing leaves no trace – victim receiver doesn't know it's being spoofed
- Spoofer typically targets a single receiver
- Many countermeasures to jamming are ineffective against spoofing

---

# Assessing the Threat

- Multi-frequency, multi-system receivers inherently resistant to spoofing
- Vast majority of GPS receivers in critical applications are single-frequency L1 C/A (easily spoofable)
- Software radio techniques are game-changer, enabling one to “download” a spoofer
- Strong financial incentives encourage “complicit spoofing” (spoofing one’s own receiver)
- Timing receivers used in communications infrastructure are attractive target

# Civil GPS Spoofing Testbed at UT Austin

## Spoofers

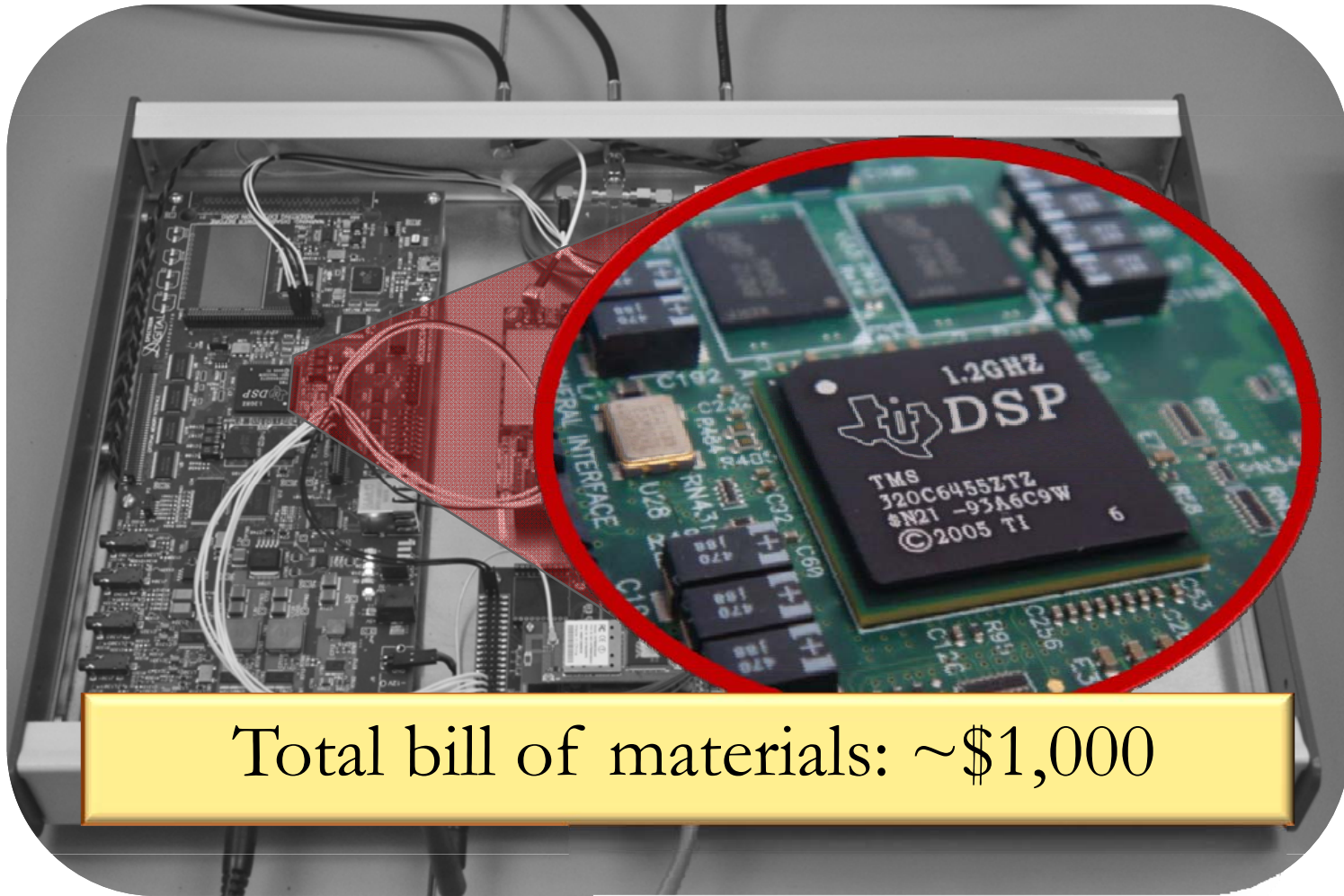
## Defender



- GPS L1 C/A output
  - Software radio platform
  - Output precisely synchronized with authentic signals via feedback
  - Finely adjustable output signal strength
  - Remotely commanded via Internet
- Vestigial signal defense
  - Data bit latency defense
  - Cryptographic defenses
  - Phase trauma monitoring
  - Dual-frequency tracking

# Inside the Box

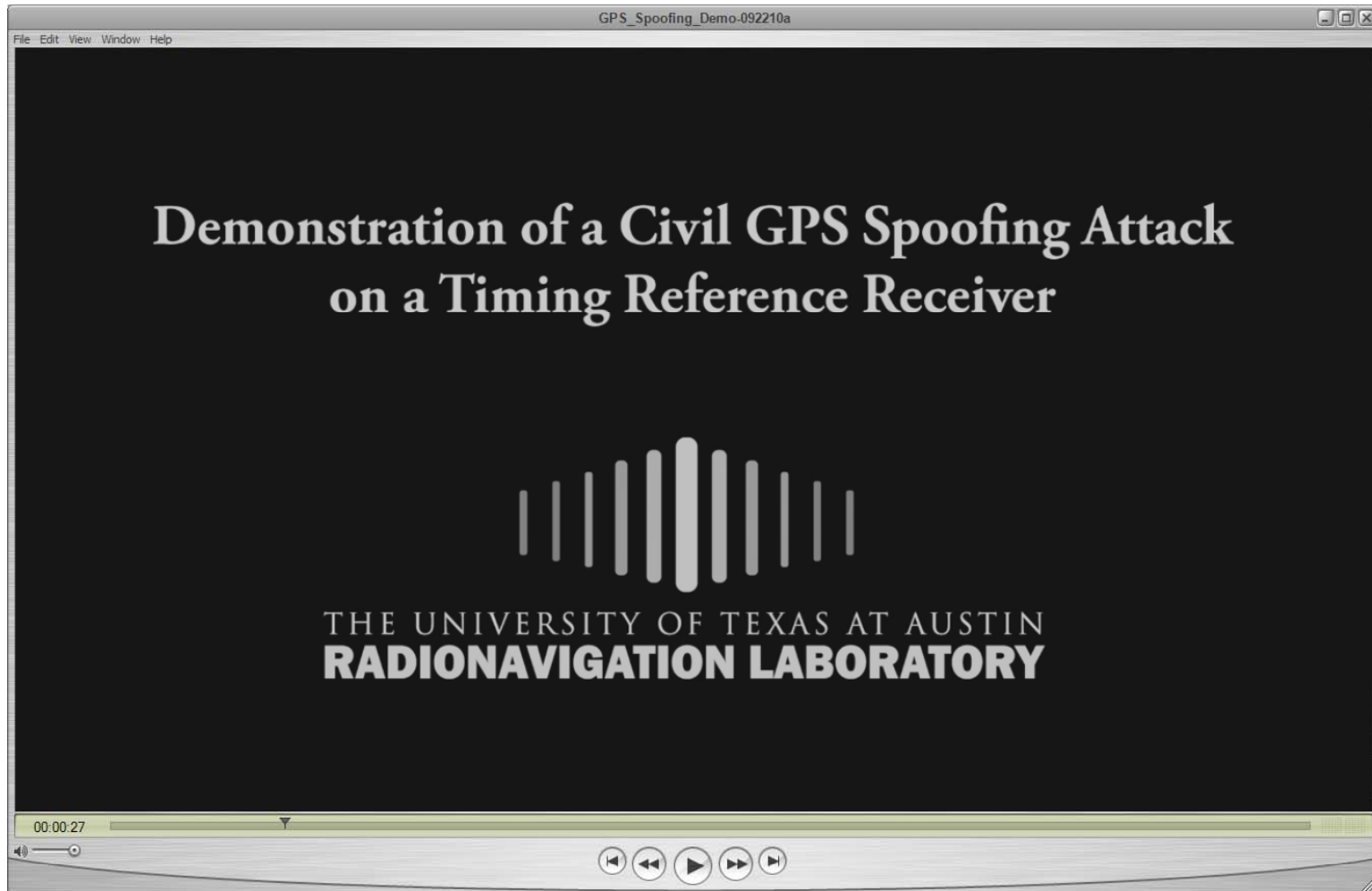
Software-defined spoofer running on COTS components



Total bill of materials: ~\$1,000

# Video Demonstration of Spoofing Attack

(<http://radionavlab.ae.utexas.edu/index.php/videos>)



---

# Observations

- “Flywheel” capability of GPS timing receivers protects against jamming but not spoofing
- CDMA cell phone base stations can be disabled within about 1 hour; power grid PMUs in less time
- J/N meters in receiver front end are essential for spoofing detection
- Practical backward-compatible spoofing defense: Navigation Message Authentication on GPS CNAV data stream (even effective against replay attacks if properly implemented)



---

# More Information

<http://radionavlab.ae.utexas.edu>