Argonne NATIONAL LABORATORY | Nuclear Engineering Division

Assuring the Veracity of Monitoring Data

See RG Johnston, MJ Timmons, and JS Warner, *Science & Global Security* 15, 185-189 (2007).

Conventional Techniques Are Not Secure

When data is logged in the field, such as with GPStrackers or nuclear safeguards monitoring equipment, it is not safe from tampering because:

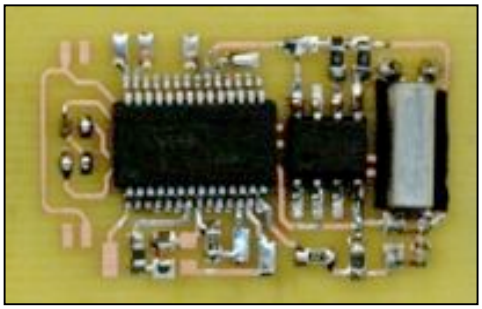
1. Conventional physical/electronic tamper and intrusion detection techniques are too easy to defeat (as shown by the Argonne Vulnerability Assessment Team and others).
2. The encryption or data authentication key cannot be erased quickly enough, even if intrusion is detected.
3. The encryption or data authentication key cannot be erased reliably enough, even if intrusion is detected, because of data remanence problems.
4. A sophisticated adversary can break the cipher even without knowing the key because he has knowledge of the algorithm and all or some of the plaintext.

OPODS: A Better Approach

OPODS stands for "Onetime Pad of Digit Substitutions". It is a stream cipher based on the only unbreakable cipher—the one time keypad.

Advantages include:

- Much better security than conventional ciphers or MACs when physical security & tamper detection is poor (as is usually the case).
- Data recorded prior to trespassing cannot be modified; data after trespassing is not as secure but is difficult to fake.
- The data is quite secure even if the trespassing or tampering goes undetected.



- It's a fast algorithm (not computationally intensive).
- Cheap & easy to implement on low-cost microprocessors.
- Only 1-2 bytes need to be quickly and reliably erased once intrusion is detected, not 256 bytes or more as is the case with a conventional high-security key.
- The technique has been demonstrated on notebook computers and small microprocessor circuits.
- Works with analog or digital data.

Applications

- courier bags
- safe & vault logs
- audio recordings
- GPS data logging
- tamper detection
- nuclear safeguards
- counter-intelligence
- weapons use logging
- financial transactions
- biometrics & access control devices

CONTACT > Roger G. Johnston, Ph.D., CPP | 630-252-6168 | rogerj@anl.gov | Nuclear Engineering Division | www.anl.gov