Links and References

1. FIPS 140-1 and 140-2 validated devices: http://csrc.nist.gov/cryptval/140-1/1401val.htm
2. FIPS Cryptographic Module Validation (CMV) Program: http://csrc.nist.gov/cryptval/
3. TAMPER Lab. http://www.cl.cam.ac.uk/Research/Security/tamper/
4. 2600.com. http://www.2600.com/
5. D. Aucsmith. 'Tamper Resistant Software'. Proceedings of the first information hiding workshop, Cambridge, England 1996.
6. Boaz Barak, Oded Goldreich, Rusell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, and Ke Yang. On the (Im)possibility of Obfuscating Programs. http://www.wisdom.weizmann.ac.il/~oded/p_obfuscate.html
7. A paper on differential fault analysis on symmetric key schemes: http://www.cs.technion.ac.il/~biham/publications.html
8. A paper on attacking crypto protocols by hardware failure: http://crypto.stanford.edu/~dabo/abstracts/faults.html. Note that this kind of technique may be used to attack physical tamper-resistant hardware such as smart cards (mentioned in the above paper 7.).
9. http://www.webcrunchers.com/crunch/esq-art.html. **NB**: It is strongly recommended (but not required) that you read this fun page about the history of attacks on phone systems.