Shoddy Spares Customer Circumvention

18-849b Dependable Embedded Systems

John DeVale

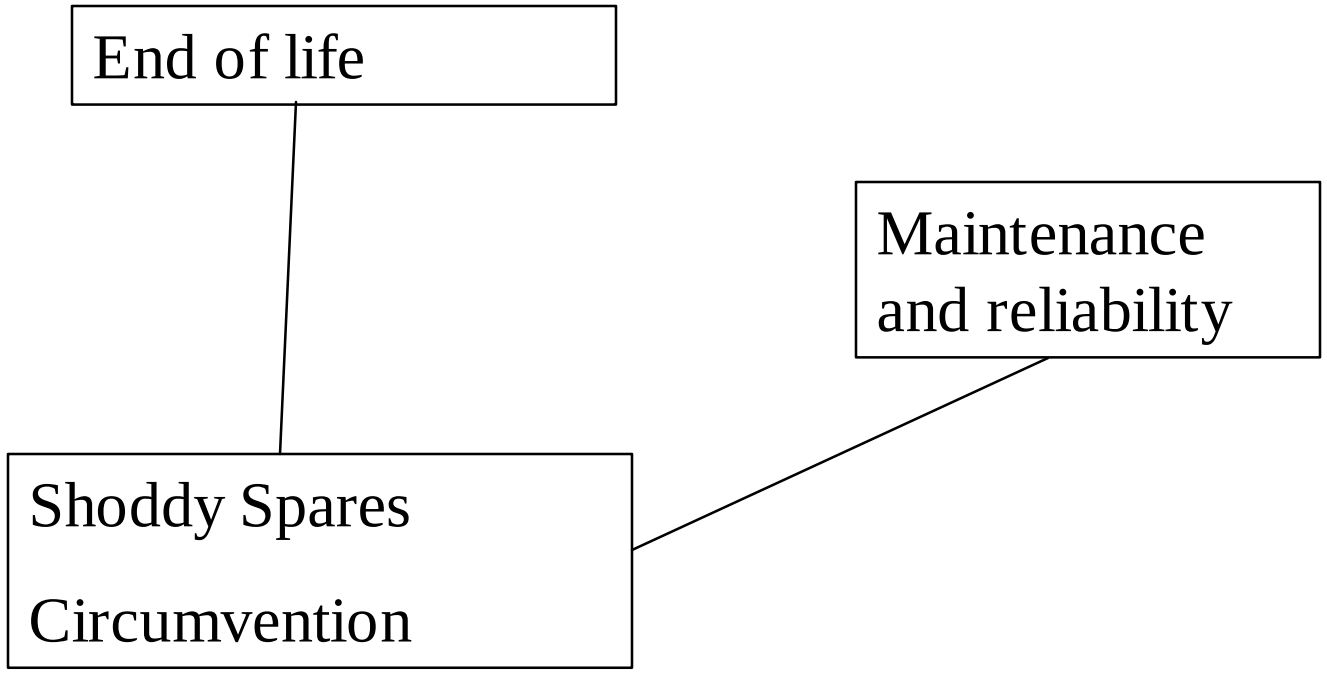
April 1, 1999 (no kidding)

Carnegie Mellon

Overview: Shoddy Spares, Customer Circumvention

- **Introduction**
  - Any design should take into consideration a customer's desire to save money, or bypass safeties in the name of expediency
- **Key concepts**
  - Security/Authentication
  - Safety/Reliability
  - Regulations
- **Tools / techniques / metrics**
  - None, but design for security
- **Relationship to other topics**
  - Reliability
  - Wearout
- **Hard to do, people are clever**

YOU ARE HERE MAP



Description of Topic

- **Shoddy Spares**
  - Fake, or cheap parts used in systems during maintenance
- **Security/Authentication**
  - Many security schemes based in hardware/software that is user-accessible can and will be bypassed
- **Safety/Environmental**
  - Similarly, safety or environmental systems which are “inconvenient” can by bypassed
- **Regulations**
  - Systems bypassed or compromised by shoddy spares can compromise compliance with safety/environmental regulations

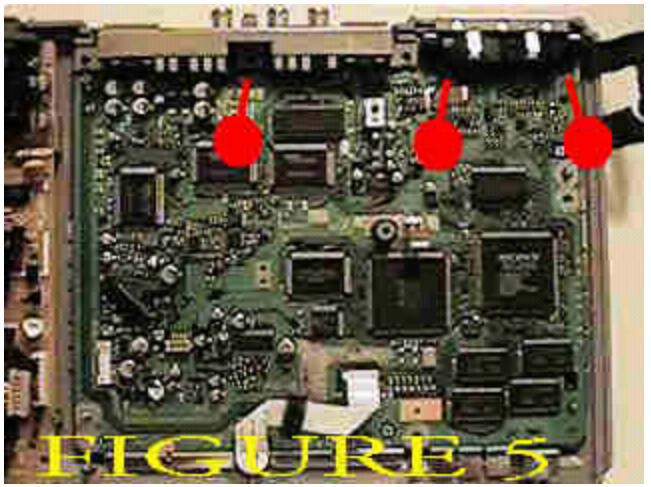
Shoddy Spares

- **Maintaining a complex engineered system is expensive. Corporations and individuals can save money by using replacement parts which do not meet specification, or are counterfeit - they are “shoddy”, but less expensive.**

- **Counterfeit parts cost US industry an estimated 500 million in 1986 [Cohen 88]. Similarly, the software industry claims $11.4 Billion in losses due to piracy and counterfeiting in 1997[spa 97]**

Security/Authentication

- DIVX - relies on hardware and software built into the DVD player which charged the user's account for playing DIVX encoded digital video discs
- DVD - Read country code on disc and in the player to determine the geographic location, and if it should play the disc
- Sony Playstation, reads copy protection sector off CD-Rom discs

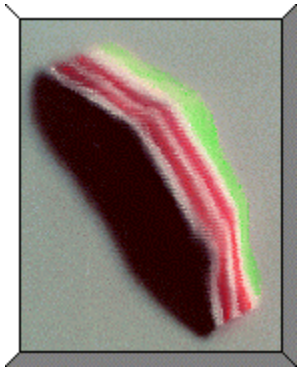


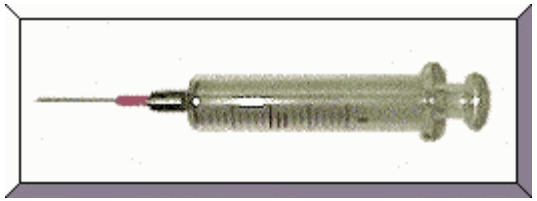
Safety/Environmental

- **1986 Enstrom F-28 Helicopter crashes killing reporter Jane Dornaker. Cause tied to counterfeit parts [fortune 87]**
- **President of Execuair Corp convicted of selling counterfeit parts to USAF in 1986 [fortune 87]**
- **Nortwest Flight 520 crashed during takeoff, one factor listed is that the warning system telling pilot the flaps were incorrectly positioned was disabled [NTSB 87]**
- **Vehicle performance chips enhance power at the expense of fuel use and excess exhaust [superchips 99]**

Tools / Techniques

- **Microtaggants [www.microtaggants.com]**
  - microscopic particles with unique magnetic signatures
  - algorithmically calculate serial number from signature
  - If match, part is genuine
  - Caveat: requires cryptographicly secure algorithm, and (physically) secure software. May not work for intentional circumvention





Relationship To Other Topic Areas

- **Reliability (general**
  - reliability of any system can be compromised by using shoddy spares
- **End of life/wearout**
  - systems without certified components will most likely not function according to design
- **Certification**
  - Certification only good for system as designed, deviation will void certification

Conclusions & Future Work

- **Shoddy spares - if intentional still pose a challenge. Most any system can be compromised if there is no physical security**
- **Circumvention is equally difficult, degenerating into a security problem**
- **Some industries undergo periodic review and re-certification (air, nuclear)**
- **While some tools exist, they are not iron-clad**