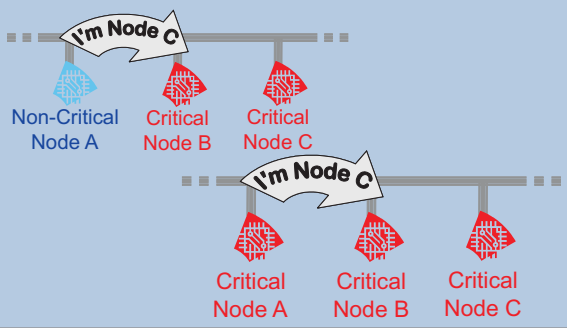
Carnegie Mellon ENGINEERING | Institute for Complex Engineered Systems | Electrical & Computer ENGINEERING | GM | BOMBARDIER TRANSPORTATION | RoSES

SOFTWARE DEFECT MASQUERADING

Jen Morris, Phil Koopman

Motivation:

- Embedded systems with a shared network
  - Mixture of critical & non-critical nodes
  - Typical design assumption: “Trust any message from a critical node”
- System defects (software, hardware) can lead to masquerading
  - Masquerading of critical nodes may compromise critical systems



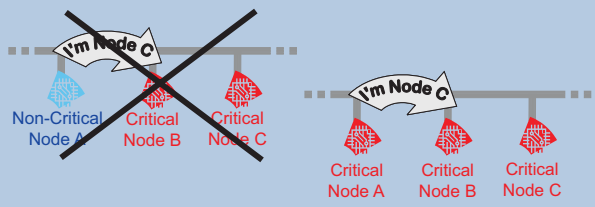
Previous Solutions:

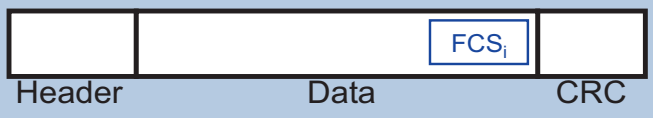
- Network-provided or Application-level CRCs
  - \+ Effective against random bit errors (noise) & some networking defects
  - \+ Inexpensive (bandwidth, processing, memory, etc.)
  - − Vulnerable to masquerading due to design defects & malicious attacks
- Symmetric & Asymmetric Digital Signatures
  - \+ Effective against design defects and malicious attacks
  - − Expensive (bandwidth, processing, memeory, etc.)

Our Technique:

Application-Level CRC with Secret Polynomial/Seed

\+ Protects against non-malicious masquerading by non-critical sources
\+ Same cost as application-level CRC
− Still vulnerable to non-malicious masquerading by critical sources
− Still vulnerable to malicious attacks

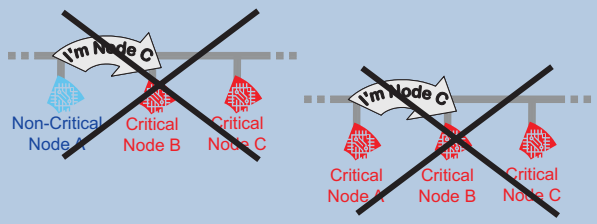




- Unique CRC polynomial CRC_i
  - $FCS_i = CRC_i(M,S)$
- Unique CRC seed value S_i
  - $FCS_i = CRC(M,S_i)$

Asymmetric Application-Level CRCs

\+ Protects against non-malicious masquerading by critical sources
− Cost of application-level CRC plus cost of signature X
− Still vulnerable to malicious attacks



- Sending process appends signature X:
  - $FCS = CRC_{i,1}(M)$
  - $X = CRC_{i,2}(FCS)$
- Receiving process verifies that:
  - $CRC_{i,1}(X) = FCS$

FCS = Frame Check Sequence M = Message i = criticality level (by message type, by node, etc.)
$CRC_{i,1}$ = Public CRC polynomial $CRC_{i,2}$ = Private CRC polynomial (inverse of $CRC_{i,1}$)

Ongoing Research:

- Analysis of commercial safety-critical networks
  - Masquerading in event-triggered and time-triggered domains
  - FlexRay, TTP/C, TTCAN, TCN, Embedded IP
- Application of techniques from train to automotive