Securing Software Stacks in Embedded Systems

Software security and system resiliency against vulnerability exploitation has seen a huge evolution in the past 10 to 15 years. While desktops and server systems have seen their level of resistance to attacks (e.g., buffer overflow attacks) improved, this is not true at all for most embedded systems. Security in embedded systems mostly focused on performing secure cryptographic computation (e.g., resistance to side channels and faults attacks) or to secure very small and closed platforms (JavaCard). On the other hand there is an important need for techniques that can be applied to embedded devices that are not security devices but devices we have to rely on nevertheless. Such devices often cannot afford high end hardware security measures or have to provide many features, making code bases larger and security more difficult. Finally, the hardening techniques available in general purpose systems are often difficult to port to embedded systems, either they need to be adapted or new techniques needs to be designed taking those as inspiration. This thesis addresses this problem by exploring techniques for symbolic execution for software testing in embedded devices.