API-Level Attacks on Embedded Systems

Mike Bond Ross Anderson

2nd May 2001

Abstract

A whole new family of attacks has recently been discovered on the application programming interfaces (APIs) used by security processors. These extend and generalise a number of attacks already known on authentication protocols. The basic idea is that by presenting valid commands to the security processor, but in an unexpected sequence, it is possible to obtain results that break the security policy envisioned by its designer. Such attacks are economically important, as security processors are used to support a wide range of services, from automatic teller machines through pay-TV to prepayment utility metering. Designing APIs that resist such attacks is difficult, as a typical security processor needs a substantial command set with several dozen commands that allow it to service a number of external and internal protocols. The attacks are also scientifically interesting; preventing them may become an important new application area for formal methods and design verification tools generally.

1 Introduction

A large and growing number of embedded systems make use of security processors to distribute control, billing and metering among devices with intermittent or restricted online connectivity. The more obvious examples include:

- the smartcards used to personalise mobile phones and to manage subscribers to satellite-TV services;
- microcontrollers used as value counters in postal meters and in vending machines to prevent fraud by maintenance staff; and
- cryptographic processors used in networks of automatic teller machines (ATMs) and point-of-sale equipment to encipher customers' personal identification numbers (PINs).

Behind these visible applications there may also be several layers of back-end systems which must prevent fraud by distributors, network operators and other participants in the value chain.

A good example is given by the prepayment electricity meters used to sell electric power to students in halls of residence, in the third world, and to poor customers