A Modern View of Smart Cards Security

Ilya O. Levin

D'Crypt Pte Ltd • ANSES RahRah 8

“Smart cards are reliably secure and are hard to attack”

Traditional View

A standalone target

Attacker is whoever have found a lost card

Modern View

A part of a complex system

Highly motivated and determined attackers

Determined Attackers

Multiple attack vectors

Plenty of time and resources

Skilled

Smart cards are vulnerable when used in a controlled hostile environment.

User PIN

Extract from a compromised user system (pkcs11.dll, usbsniff.sys, ...)

Lazy dictionary attack

Why bother at all, just run the evil stuff in background

Administrative Key

Extract from a card issuer's compromised system; disgruntled employees as a bonus

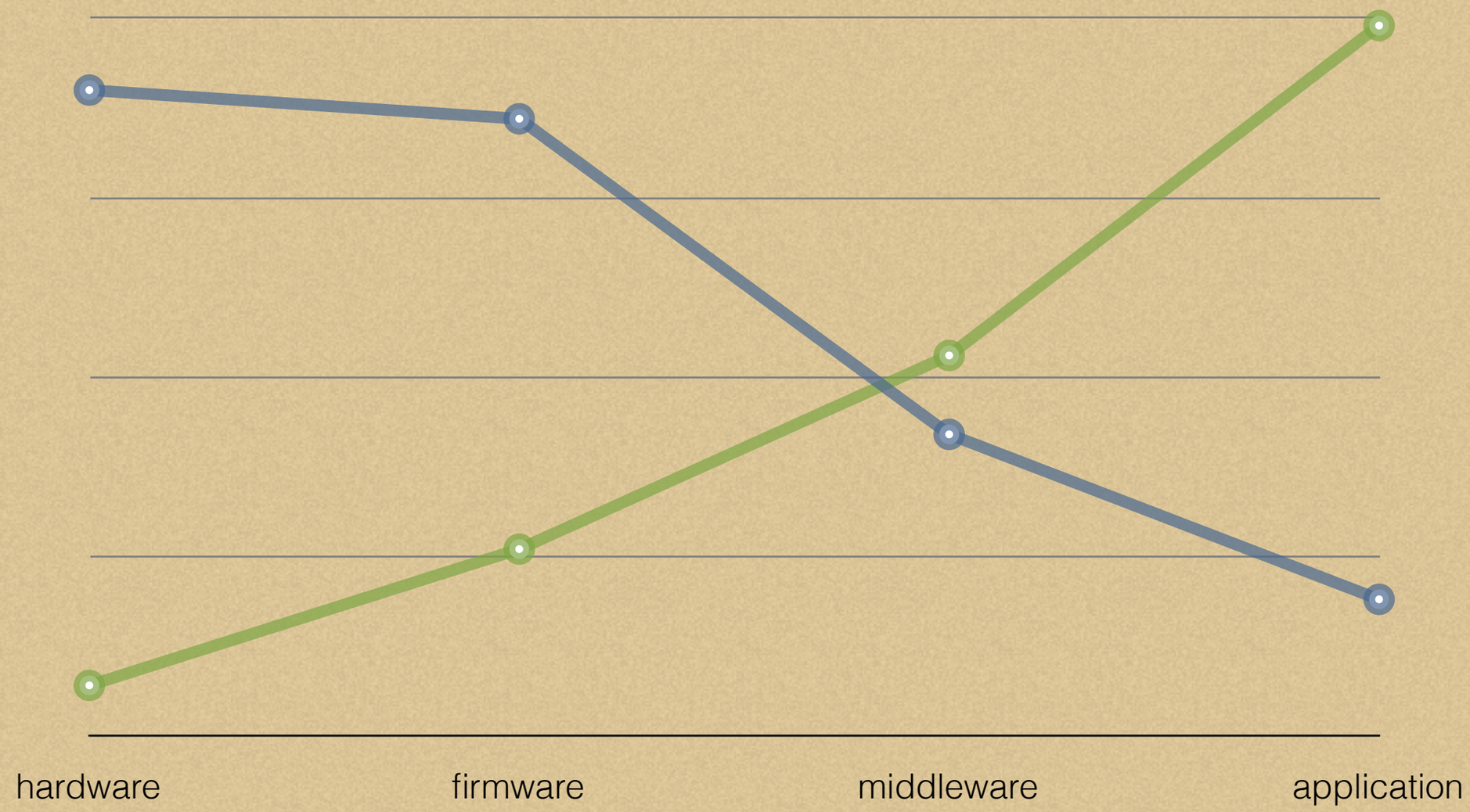
Default values

F(serial_number)

"A compromised system of a security vendor?!
Never going to happen!"

Well, hello RSA Technologies and Comodo

Skills vs Errors



Unfortunate Features

Design mistakes

Firmware implementation errors

Errors in middleware and applications

Design Mistakes

Extraction of cryptographic keys from Cryptoflex cards

The 9000 trick in Chip and PIN payment systems (Ros Anderson et al)

Firmware Implementation

Unauthorized reset of user PIN, SO PIN and card key in Charismathics plug 'n' crypt

Firmware signature check bypass with a boot loader in Kobil reader

Middleware & Applications

Forgotten reset of a card at C_Logout in GemSAFE PKCS 11

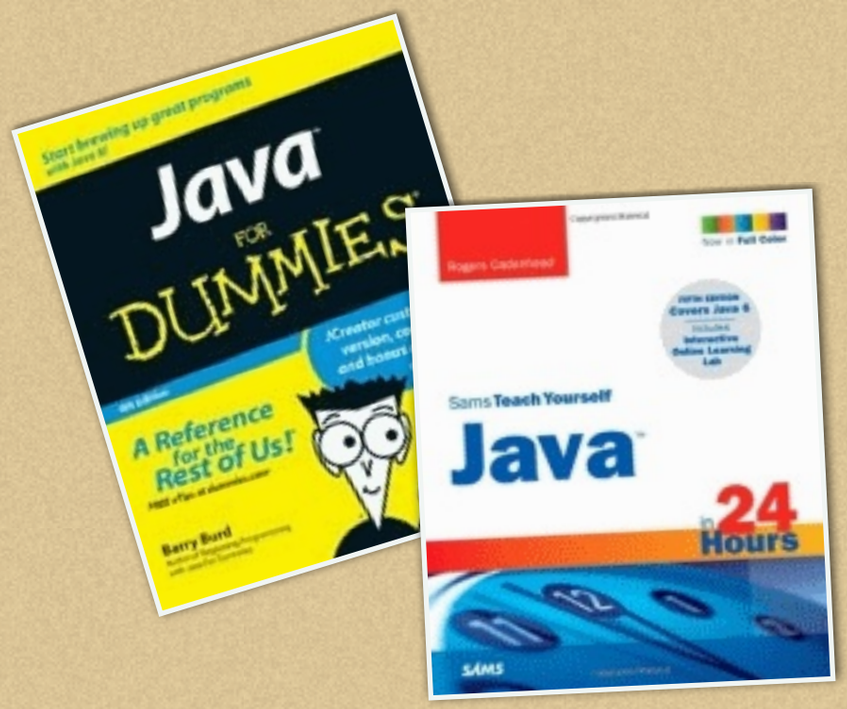
“Deleted” objects inside PKCS11 containers of Cryptoflex cards

Java Cards

Potential issues in JCVM

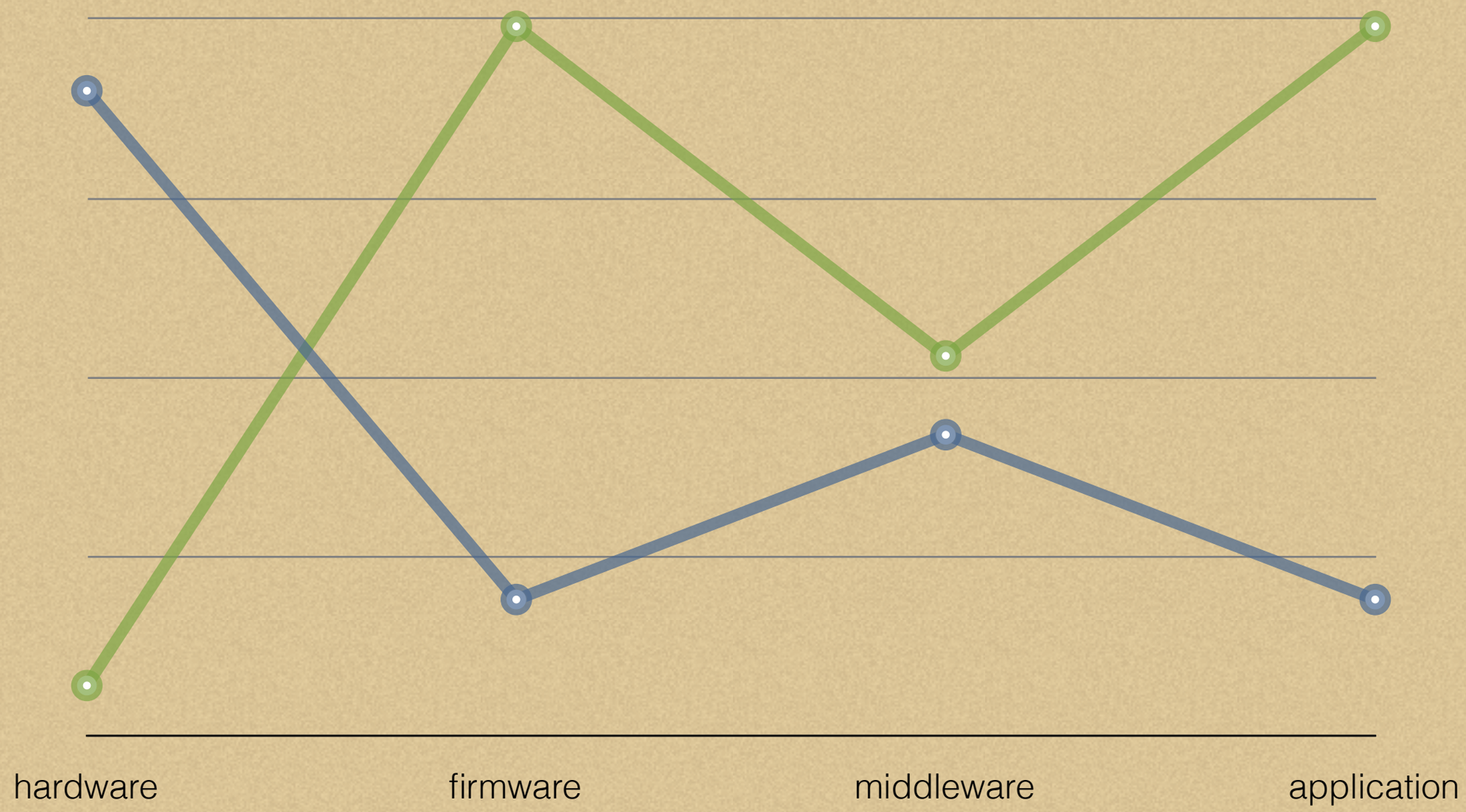
Custom written applets quality

Java Cards



"How hard can it be? It is still Java, right?"

Java Cards



Java Cards

“Hey, Java Card applets signed with trusted certificates. So, what’s a problem?”

Signatures validate authenticity, not quality

“Yeah, trusted certificates. Right” - Stuxnet

On-board Web Server

Welcome to script kiddies with ready-to-use web scanners and http fuzzers

Let's Go Contactless!

Traffic remote eavesdropping with directional antennas as additional bonus

Permanently enabled RF interface on a card as remote fuzzing target

Protiva Smart Badge Holder

Hands-free Smart Card based security for SmartPhones and PCs

The 2011 Asian SESAMES Award winner is:

Gemalto with Smart Badge Holder

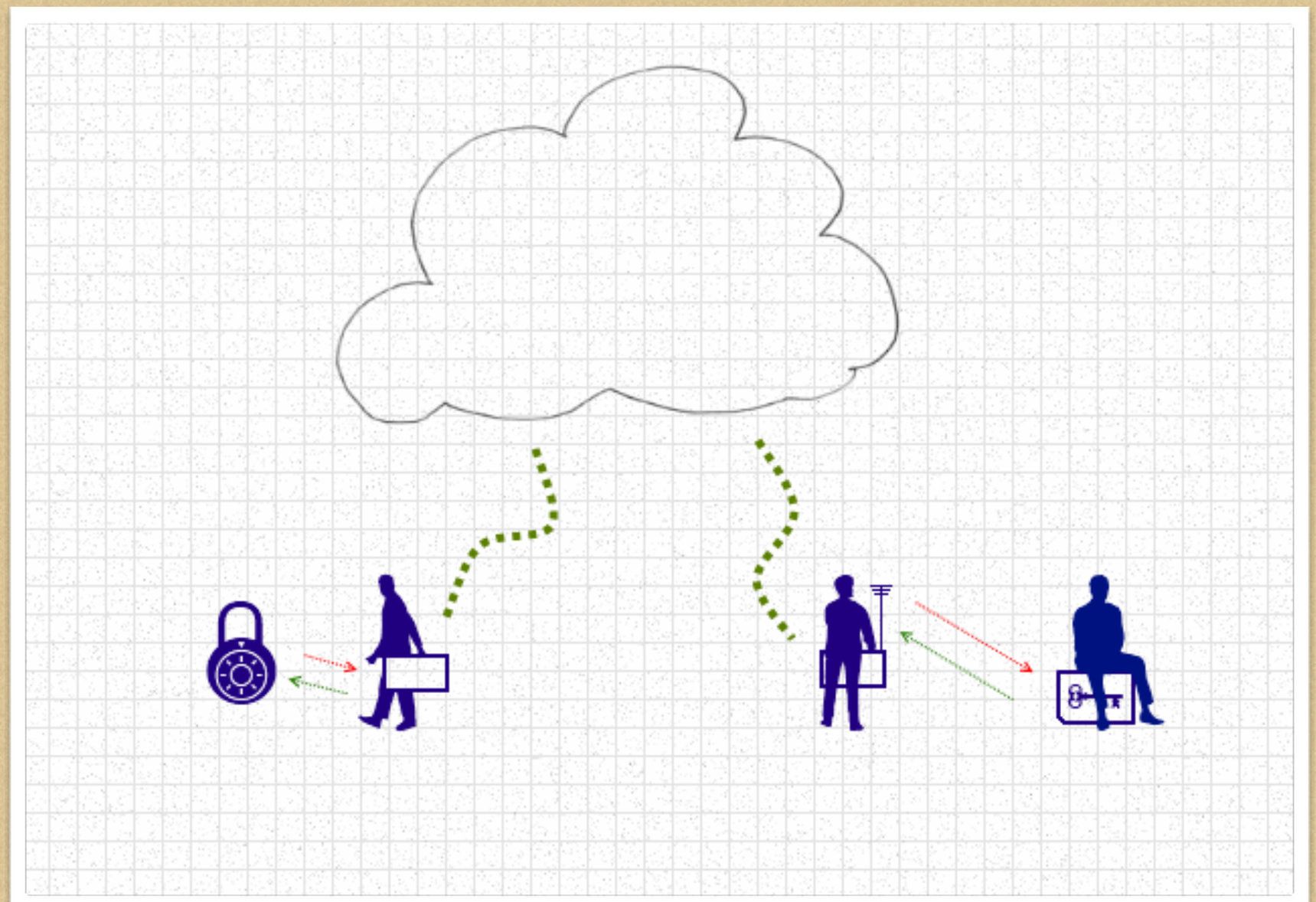
Gemalto Smart Badge Holder (SBH) – The wireless corporate badge reader solution for enterprise applications. SBH is an intelligent electronic badge holder based on Bluetooth medium distance wireless technology. It is particularly relevant for corporate applications where the corporate badge is used for logical access on small devices such as Smartphones that can't accommodate standard card readers.

Bluetooth Addendum

Chapter 4
Bluetooth Vulnerabilities, Threats, and Countermeasures

Guide to Bluetooth Security
NIST Special Publication 800-121

Radio Relay Attack



To Conclude

Smart cards are not that sound in real life as we used to believe

Bad guys are ahead of industry at the moment

We need to catch up

Thank you.