Moore’s Law and Publishing

Ross Anderson

Cambridge

What changed 2001–8?

- Many new protocols and system mechanisms fielded (AES, 3g, EMV, HomePlug, BitLocker…)
- ‘War on Terror’ leads to hypertrophy of security-industrial complex …
- How can we measure it?

WILEY

Security Engineering

Ross Anderson

SECOND EDITION

A Guide to Building Dependable Distributed Systems

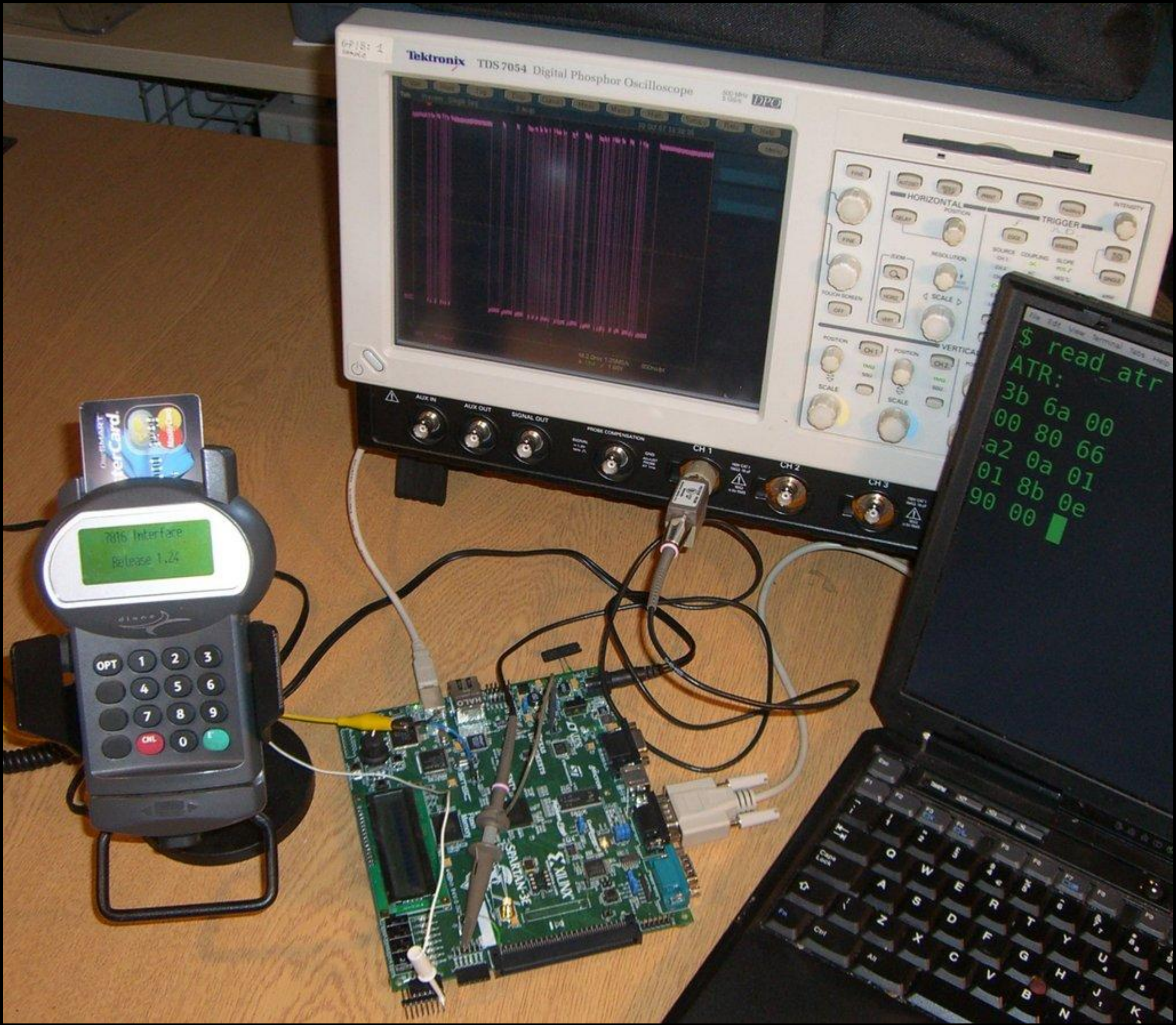
Subject growth

- Overall 62% (from 640 pages to 1040 pages) especially topics surrounding crypto:
  - Crypto implementation
  - New protocols / APIs
  - Applications
  - Real-world attacks
  - Usability
  - Policy / economics
- Increasingly these come together…

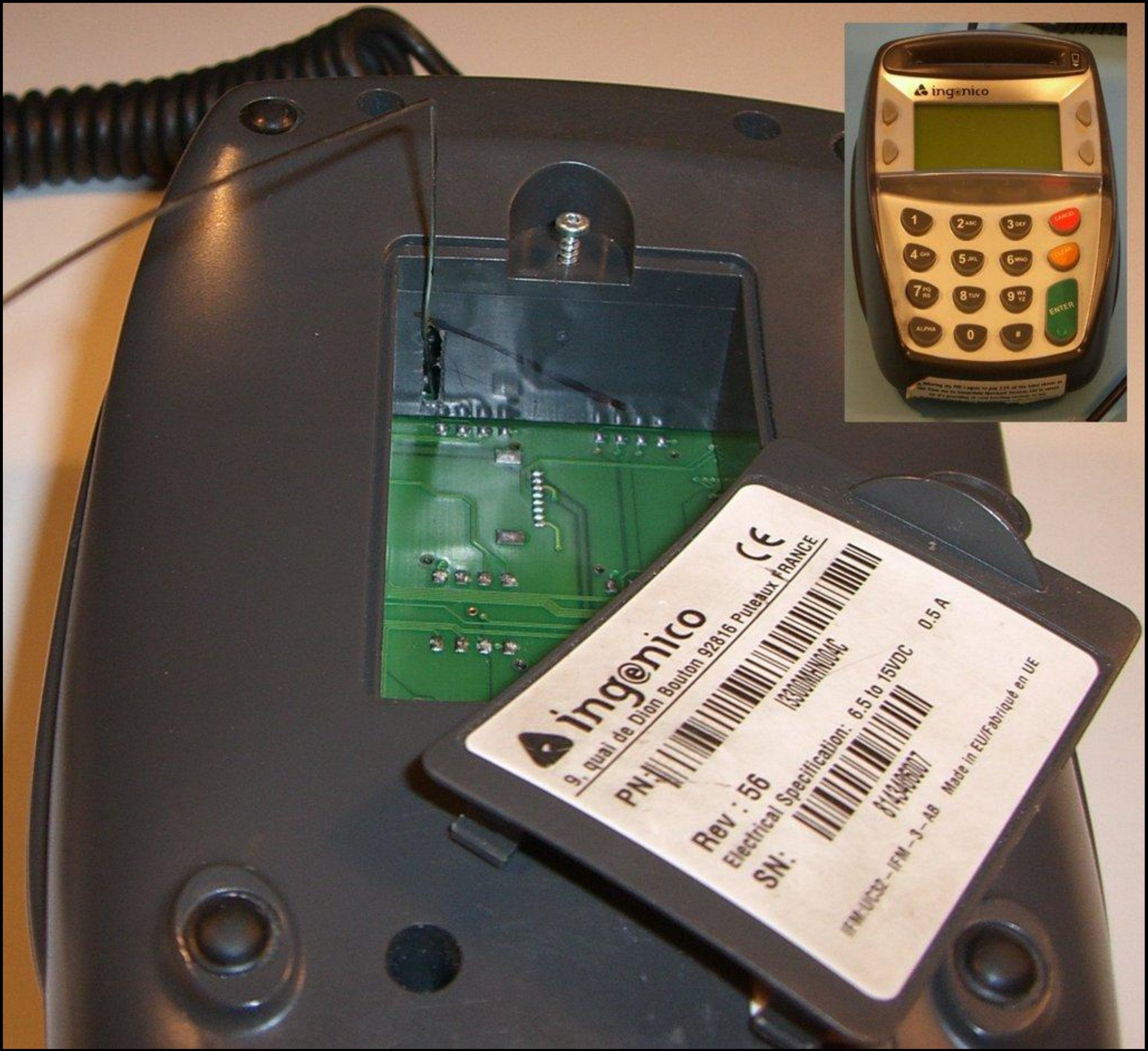
Example – breaking EMV

- Work with Saar Drimer, Steven Murdoch, to appear at Oakland next month (in book too)
- No less than 67 vendors sell ‘approved’ ‘secure’ terminals for chip and PIN
- Every one we’ve examined, we’ve broken
- This raises serious questions about the Common Criteria, and much more

dione
OPT
1
2
3
4
5
6
7
8
9
CNL
0
ENT
J7
J4
C5
J8
Designed by Dione plc
Prod Pack: XTHS1
*00201140

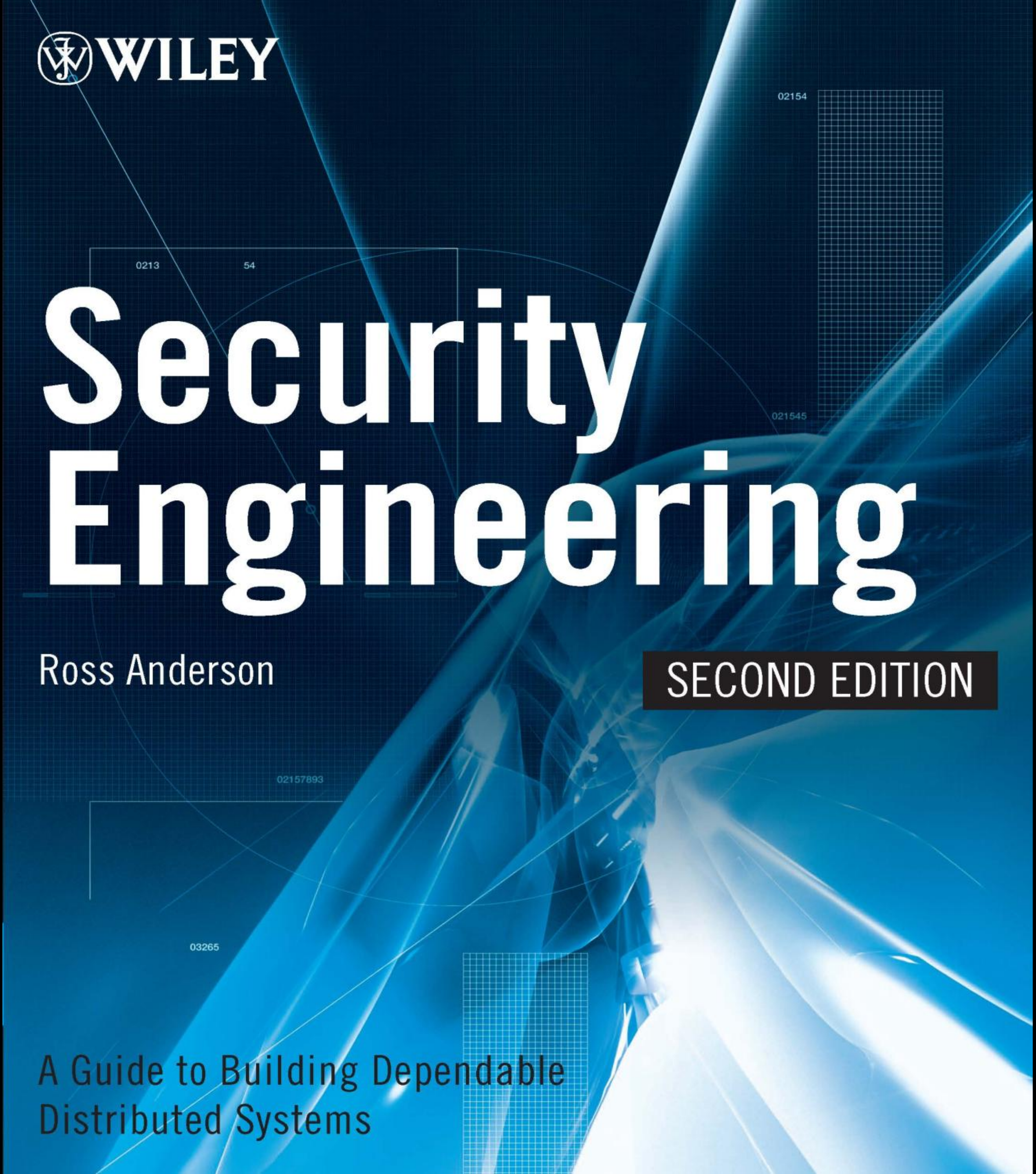


```
$ read_atr
ATR:
3b 6a 00
00 80 66
a2 0a 01
01 8b 0e
90 00
```


ingenico
9, quai de Dion Bouton 92816 Puteaux FRANCE
PN:
I3300MHN004C
Rev : 56
Electrical Specification: 6.5 to 15VDC 0.5 A
SN:
81434050007
IFM-UC32-IFM-3-AB
Made in EU/Fabriqué en UE
ingenico
CANCEL
CLEAR
ENTER
ALPHA

Published two weeks ago!

www.ross-anderson.com



WILEY

Security Engineering

Ross Anderson

SECOND EDITION

A Guide to Building Dependable Distributed Systems