

Distributed Computing: Introduction

Doug Tygar
IS 206
26 August 1999

Factors on distributed computing

- Communities
- Applications
- Services
- Business environment
- Government regulation

Government regulation of electronic commerce

- Can government regulate e-commerce issues?
- Security time moves *faster* than internet time
- Issues:
 - Systemic attacks
 - Rapid response to new types of attacks
 - Assignment of liability
 - Private vs public regulation

Security and safety concerns

- Difficult to get right
- Hard for users/consumers to evaluate
- Can lead to monstrosities ...



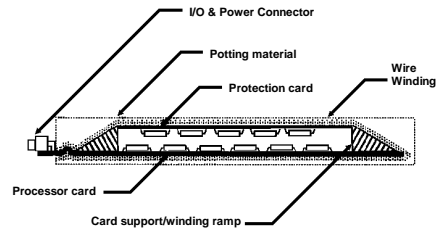
Tamper resistance & e-commerce

- Tamper resistance isolates security to single physical point.
 - Registers (available cash)
 - Cryptographic keys
 - Rights management information
 - Copy protection information
- Examples
 - Smart cards
 - Active tokens
 - Settop boxes
 - Rights management devices
 - DIVX decoders **[RIP]**
 - Dongles

Tamper-resistance

- Attempt at standard: FIPS 140-1
- Ingredients:
 - Tamperproof covering
 - If unit is penetrated, then all crucial memory is zeroed)
 - Nonvolatile RAM (register and key storage)
 - Processors and memory
 - Can store info
- Secure coprocessing O/S
 - Examples:
 - Dyad
 - Intertrust

Example: IBM Citadel secure coprocessor



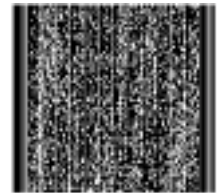
Example application: postage meters

- Postage meter fraud is rampant
 - (>\$200 million/year)
- Easy to reproduce postage meter indicia by rubber stamp, color printer, etc



Solution —secure coprocessor signs indicia

- Customer buys postage from vendor (soon, at least a dozen products may be on the market)
- Secure coprocessor
 - Securely maintains postage balance
 - Cryptographically signs indicia
- Indicia uses 2-D bar code
 - Can compress 400 - 600 bytes per square inch
- Indicia includes envelope specific info
 - Date
 - Recipient's address
 - Sender's address

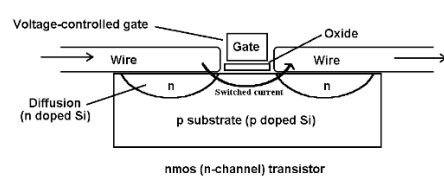


How does government regulate security?

- For most applications, no regulation!
- FIPS 140-1 problems:
 - standard for crypto devices only
 - Stretched to e-commerce & rights management
 - Government crypto only (= no RSA)
 - Evaluation by private labs, who are paid by vendors
 - Some labs invest in tamper resistant companies!
 - Avoided older military standards such as TEMPEST
 - Vendors do not accurately describe their products

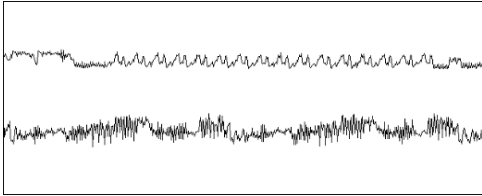
Latest wrinkle -- power analysis attacks

- Publicized by Paul Kocher et al.
- Use current drawn by device to read off cryptographic key
- Typical MOS Transistor:



Simple Power Analysis

- Can read crypto key directly from power trace



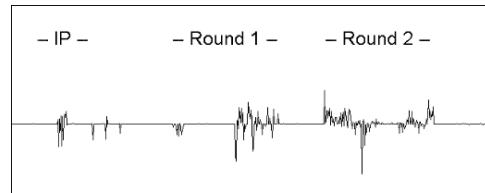
©1999 by J. D. Tygar

IS-206 slides

13

Differential Power Analysis

- Average across multiple traces to determine crypto key information



©1999 by J. D. Tygar

IS-206 slides

14

Regulatory problems

- Security presents special challenges for regulation
 - New attacks
 - Large scale systemic failures
- End users can't evaluate security risk of innovative e-commerce systems
- Liability should fall on those most able to provide enhanced security

©1999 by J. D. Tygar

IS-206 slides

15

Where are we today?

- IBM sells two top-level tamper-resistant devices
- About 40 lesser ranked devices available
- NIST now working on new FIPS 140-2 standard
 - incorporates power analysis attacks in a weak way
 - More than 2 dozen groups claim to have broken systems via power analysis
- Number of partial solutions for power analysis defense
- IBI standard for USPS
- Will become dominant form of metering

©1999 by J. D. Tygar

IS-206 slides

16