RSA CONFERENCE 2007

Failing Gracefully:
Patching & beyond

Paul Kocher
Cryptography Research, Inc.
paul@cryptography.com

www.cryptography.com

CRYPTOGRAPHY RESEARCH

Brief Bio

- Founded Cryptography Research, Inc. 11 years ago
  - Focus on mitigating "unsolvable" real-world security problems
- Examples of projects & work by myself and the team at CRI:
  - CryptoFirewall™: Tamper-resistant hardware for securing pay TV services
  - Deep Crack: Hardware to break DES
  - DPA & countermeasures: >1 billion smartcards made annually have DPA countermeasures patented by CRI
  - SPDC™: Renewable security for optical disc formats
  - SSL v3.0 / TLS v1.0
- Designs secure >>$100B of commerce annually

CRYPTOGRAPHY RESEARCH

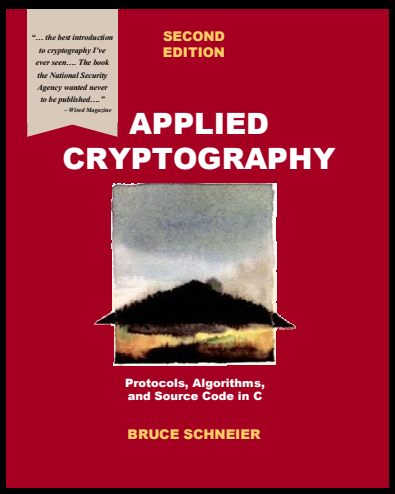
RSA CONFERENCE 2007

2

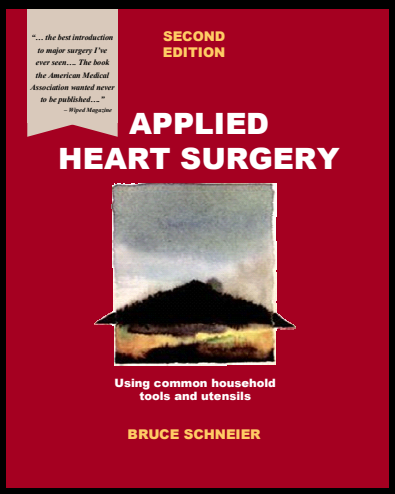
CRYPTOGRAPHY RESEARCH

We've spent ages seeking to "achieve" security…

Optimism is fading…

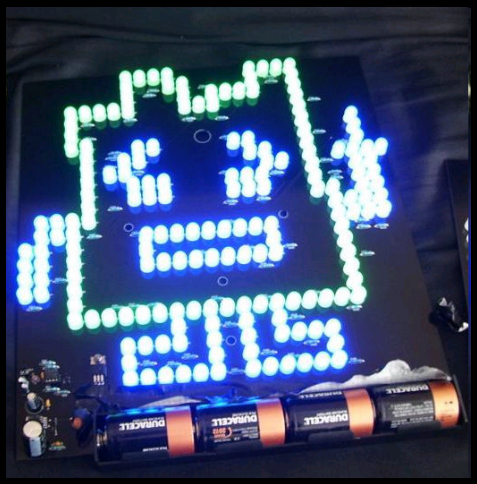


=



?

The world is filled with **scary things**!

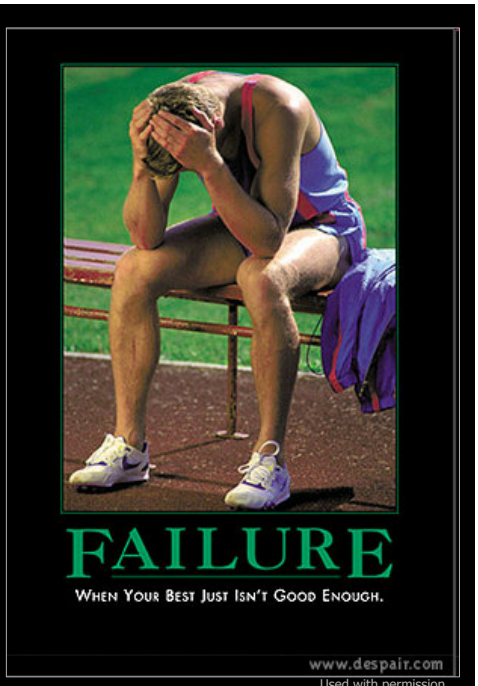


What if it's all hopeless?

What if we're doomed to an eternity of

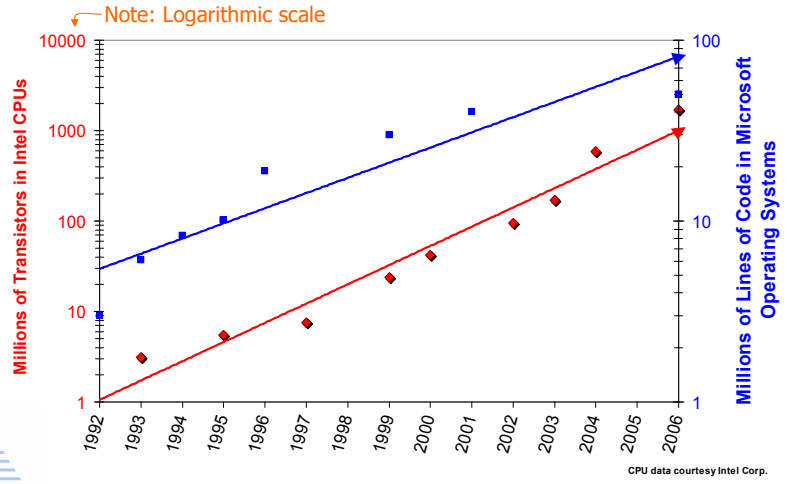
Patches

and other coping mechanisms?



Used with permission.

Growth in complexity



CRYPTOGRAPHY RESEARCH

RSACONFERENCE2007

9

Moore's Law overwhelms everything

- Tools can help buy some time:
  - Safer programming languages
  - Code scanning tools
  - Better APIs/libraries
  - Additional layers of abstraction
  - Run-time detection
  - Stack monitoring/canaries
- Certifications can also buy time:
  - Good ones help weed out the worst products and encourage good engineering
  - Bad ones drive away experienced engineers who are allergic to paperwork and detract from the real problems
  - Complexity of products is overwhelming evaluators

- Tools & certifications help by a *constant factor*
  - Addresses X% of the bugs
  - Which means there are still some bugs – and complexity inevitably catches up again…

CRYPTOGRAPHY RESEARCH

RSACONFERENCE2007

10

CRYPTOGRAPHY RESEARCH

Three coping strategies…
(Besides prayer, magic, or unlimited security budgets)

- Three strategies I'll examine:
  - On-line updates
  - Piggybacking strategies
  - Redundancy-based security architectures

CRYPTOGRAPHY RESEARCH

RSA CONFERENCE 2007

11

The Microsoft approach

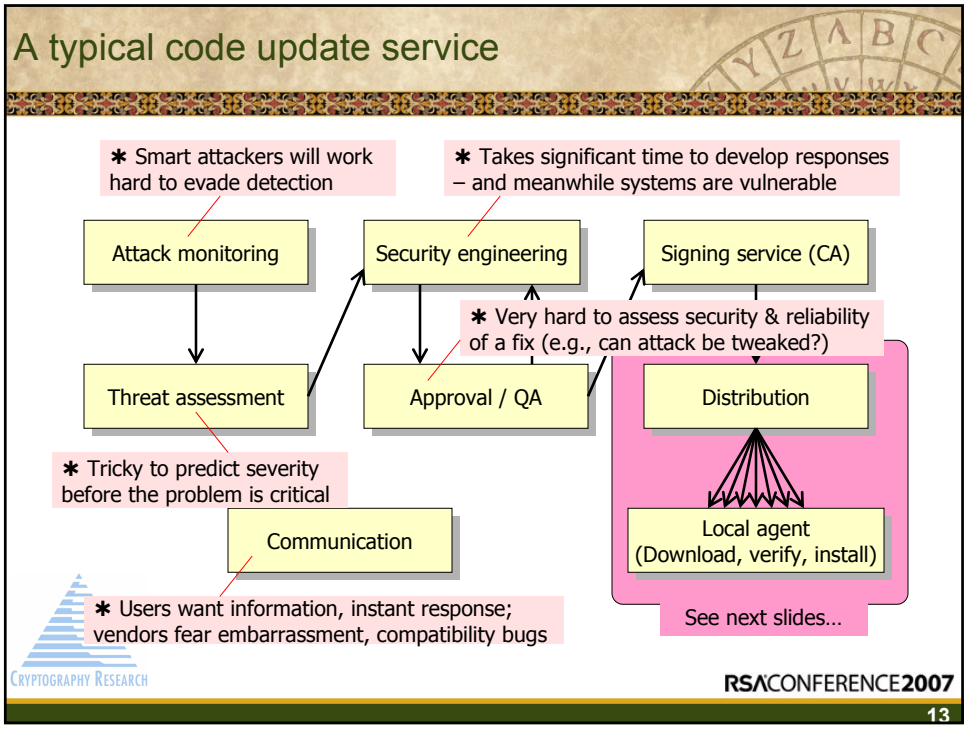
- Windows has security bugs
  - Microsoft is trying hard: Density of bugs is decreasing
  - But complexity of Windows (other ring 0 code) is increasing
- Windows-based PCs could not survive on the Internet without updates
  - Infrastructure is "worth" targeting [even if only for ego]
  - Eventually an unstoppable exploit would arrive
- Windows would be unusable without Microsoft Update

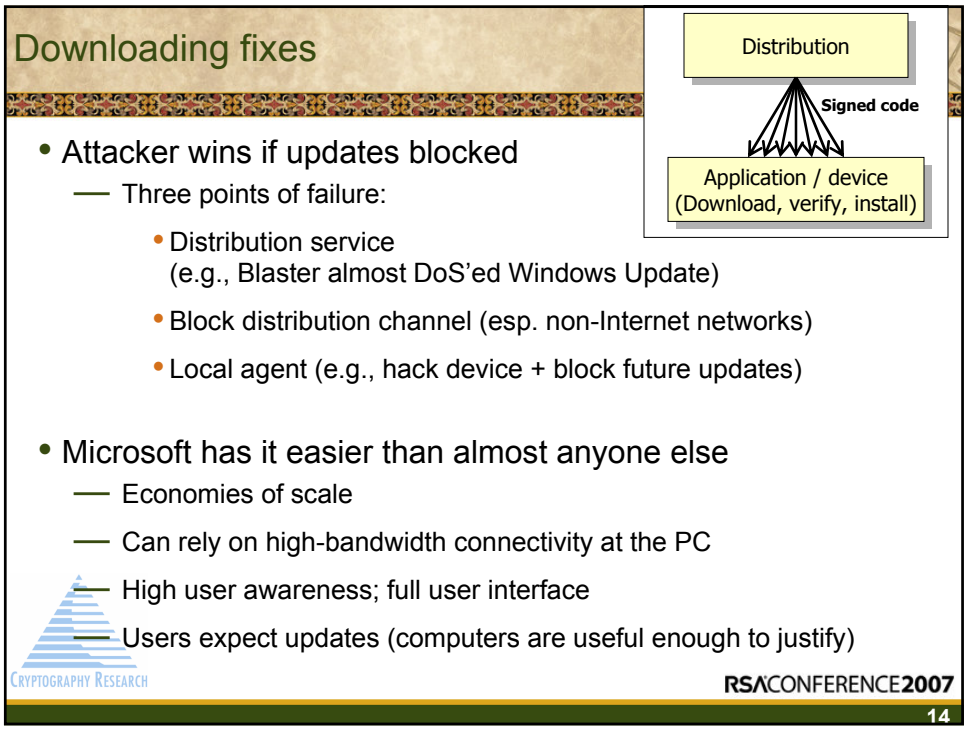
CRYPTOGRAPHY RESEARCH

RSA CONFERENCE 2007

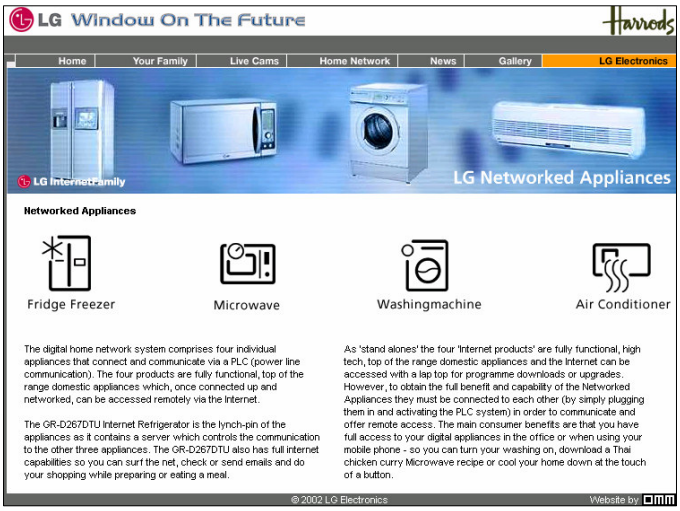
12

CRYPTOGRAPHY RESEARCH





Beyond Windows & anti-virus applications: Fixing bugs



CRYPTOGRAPHY RESEARCH

RSACONFERENCE2007

15

Beyond Windows + anti-virus applications

- Problem gets much harder
  - Limited user interface
  - Network connectivity may be expensive or unavailable
  - User expectation: Reliability (not frequent changes)
  - Product usage model does not provide convenient alternative recovery channels

User may be cooperative:

- Routers
- Firewalls
- Mobile phones
- Security Cameras
- Printers
- GPS Navigation
- VoIP phones
- Printer consumables

... or adversarial:

- Video game systems
- Pay TV decoders
- Media players
- Home Ent. Systems
- Payment cards
- ID cards/tokens

CRYPTOGRAPHY RESEARCH

RSACONFERENCE2007

16

CRYPTOGRAPHY RESEARCH

More problems (1 of 2)

- Problem: Malicious code can disable update downloader
  - Attacker goal: block the update & prevent users from noticing
    - Viruses often try this against anti-virus software
  - Strategy for devices: Update-at-boot
    - Boot flash checks over the network for updates
    - Before running other code, boot flash hardware disables writes to itself until reboot
  - Strategy for PCs:
    - Race to get the patch out before exploit
    - Force attacker to rewrite/modify a lot of (uniquely randomized) code
    - Leverage flexible user interface & user awareness

Cryptography Research

RSA CONFERENCE 2007

17

More problems (2 of 2)

- Problem: Denial-of-service on servers
  - Attacker wins if the update service is DoS'ed
  - Solution: Multiple DNS queries/IP addresses, updateable connection strategies (e.g., Java code), big pipes, priority for authenticated devices (if privacy permits)
- Problem: Patches can cause compatibility issues
  - No good solution.
    - Patches are hard to write, hard to test, and frequently cause trouble
    - Users hate them for good reason

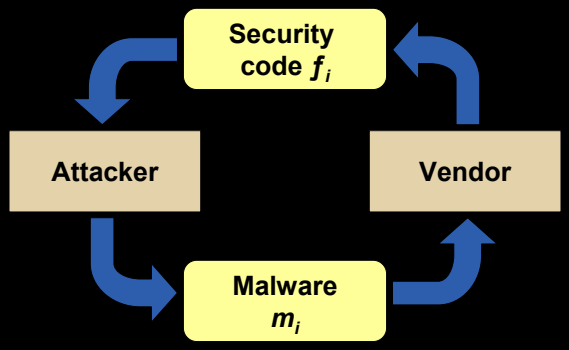
Cryptography Research

RSA CONFERENCE 2007

18

Cryptography Research

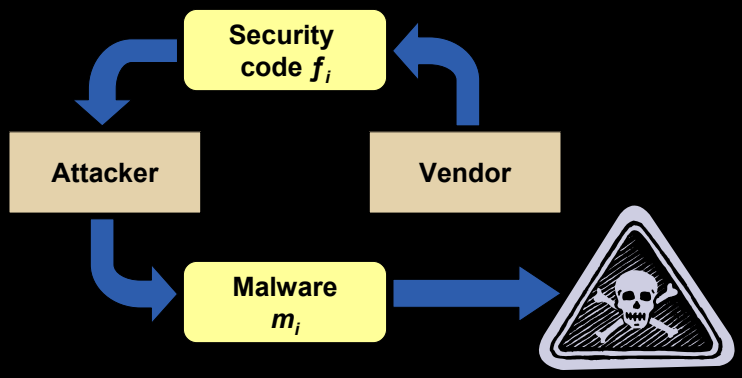
Summary of 21st Century O/S Security



CoreWars 2007

Exponential complexity growth in the environment
Users' data forms the battlefield

Summary of 21st Century O/S Security

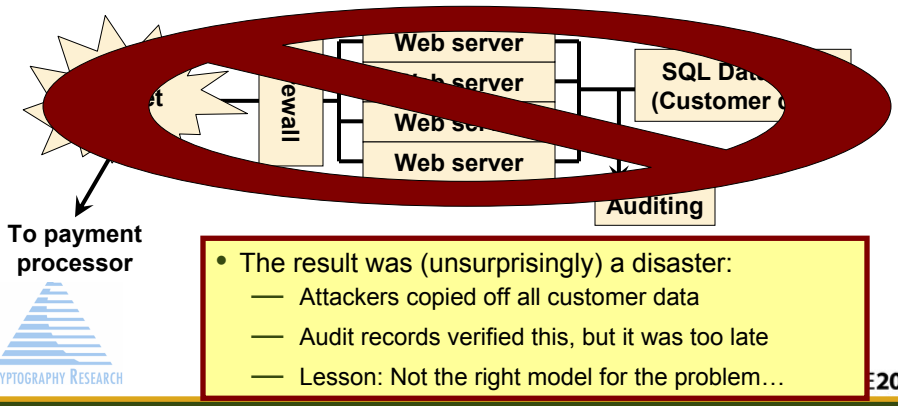


But on the bright side…

It's often less ghastly than the alternative.

Case study: Merchant e-commerce credit card database

- Running separate high-security servers for customer data is expensive and cumbersome
  - Approach: Allow web servers to access customer & payment data, but have a comprehensive audit system + stay current on patches
  - Significantly reduced costs!



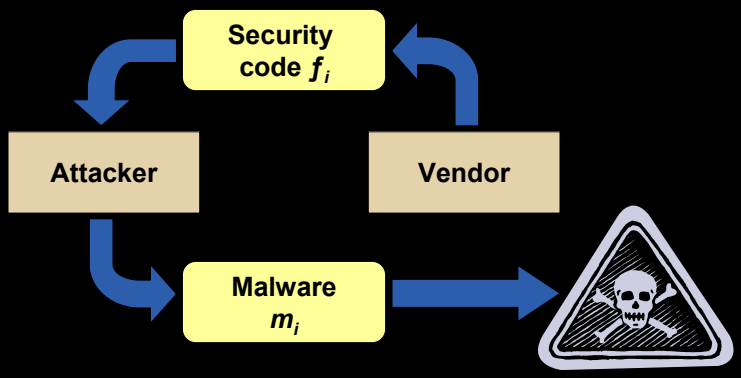
- The result was (unsurprisingly) a disaster:
  - Attackers copied off all customer data
  - Audit records verified this, but it was too late
  - Lesson: Not the right model for the problem…

CRYPTOGRAPHY RESEARCH

2007

21

Summary of 21st Century O/S Security

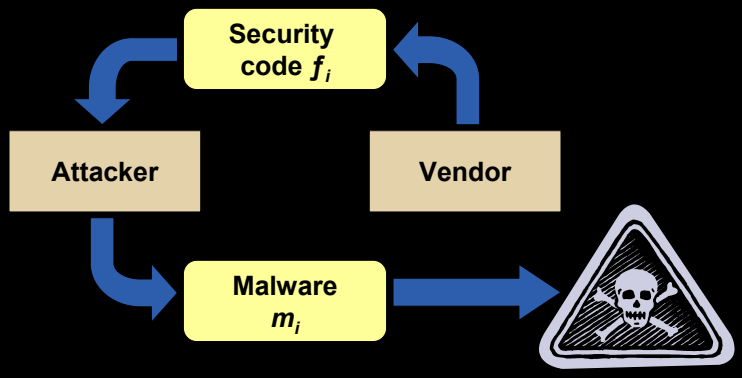


But on the bright side…

It's often less ghastly than the alternative.

CRYPTOGRAPHY RESEARCH

Summary of 21st Century O/S Security



But on the bright side…

(but not always)

It's often ^ less ghastly than the alternative.

Making the problem "less bad"

- Lots of practical issues we'd like to mitigate…
  - Do multiple vendors make device? Provides source data?
  - Are there multiple versions of target devices?
  - Bandwidth limitations? Backward compatibility issues?
  - How is customer service handled?
  - Do vendors support their devices indefinitely?
  - Will users ever miss patches? Have NVRAM bit errors? …

Cryptography Research

RSA CONFERENCE 2007

24

Cryptography Research

Piggybacking

- Many devices' normal role is to process data
  - Can include security updates as part of this data
  - Bundling with beneficial data enables security updates in adversarial models (e.g. piracy situations)

Cryptography Research

RSA CONFERENCE 2007

25

Case study: Piracy from academy screeners

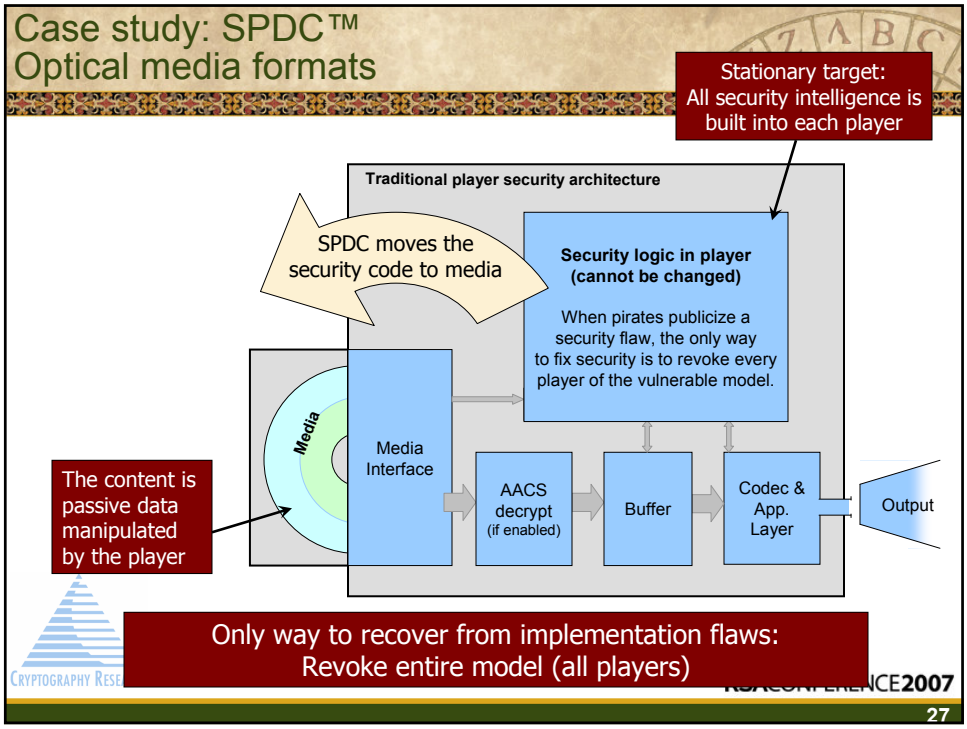
- Academy members need to see movies so they can vote on them for academy awards
  - Problem: Virtually every movie was getting pirated
  - Much too expensive & difficult to try to make movies uncopyable
- Solution: Piggybacked forensic marking data
  - Unique identifying marks in each original enable copies to be traced
- Adding a back-channel solved the problem
  - Russell Sprague went to jail; Carmine Caridi kicked out of Academy
  - Today, screeners are rarely pirated and sources get shut off quickly
  - Very successful: problem is self-limiting

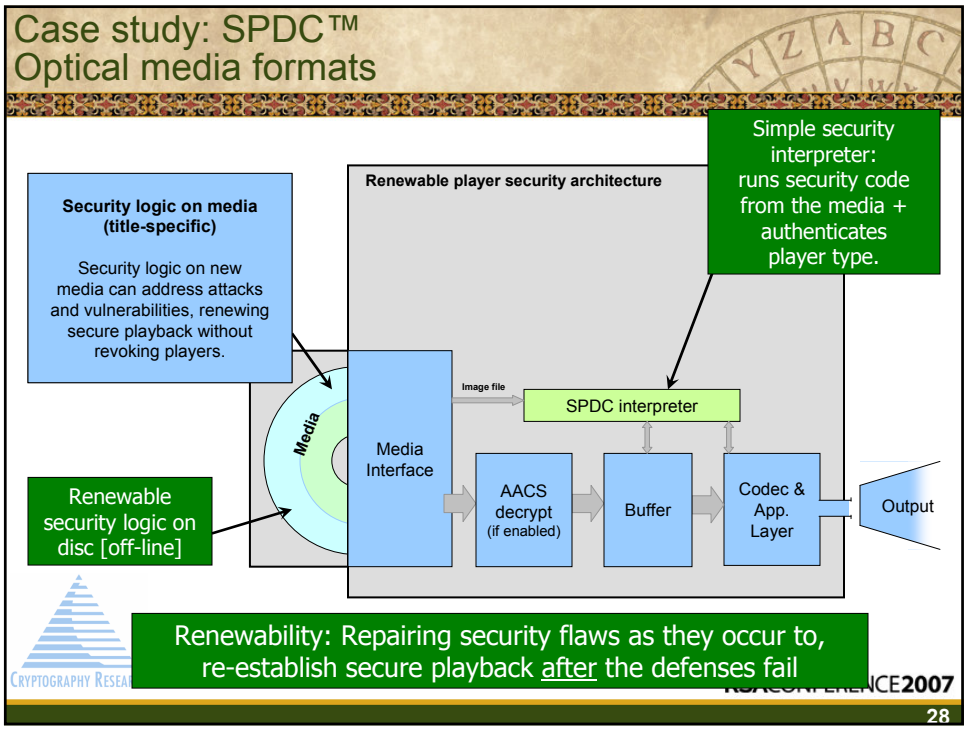
Cryptography Research

RSA CONFERENCE 2007

26

Cryptography Research

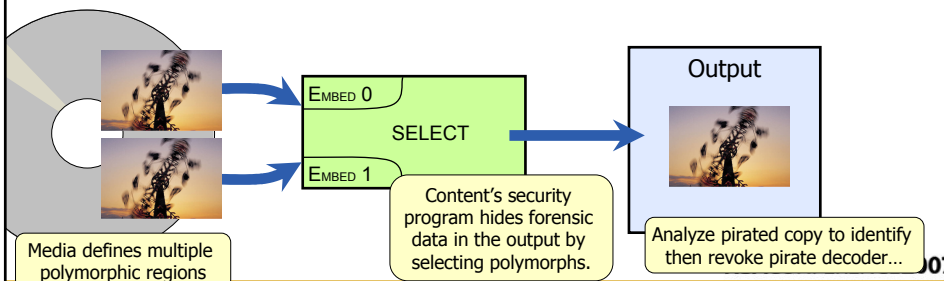




Case study: SPDC™ Optical media formats

Provided by reprogrammability

- Risk management requires knowledge and control.
- Forensic marking: Knowing what went wrong.
  - Player can allow content program to modify the output
    - Modifications may be unique to player, output devices, user, keys.
  - Addresses anonymity of piracy
    - No impact on privacy of users who don't redistribute copies.



RSA CONFERENCE 2007 29

Complexity is going to keep increasing.

Harnessing it to improve security…

Cryptography Research

RSA CONFERENCE 2007 30

Hardware architectures

- Fully-featured CPUs (such as those in smart cards) are fiendishly difficult to secure from tampering
  - Software bugs
  - External monitoring attacks
  - Invasive attacks
  - ...
- A tiny oversight… and the whole thing collapses
- A better general approach is required

  … especially as complexity increases…

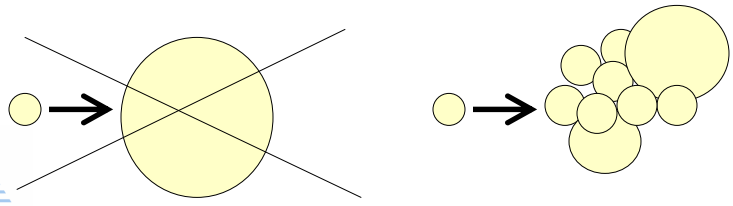
CRYPTOGRAPHY RESEARCH

RSA CONFERENCE 2007

31

CPU designs, software…

- Every 18 months we can pack twice the functionality into the same die area
- What we shouldn't do:
  - Make our existing systems more complex
  - Spend all of the circuitry on the usual stuff (pipelining, L2 caches, …)



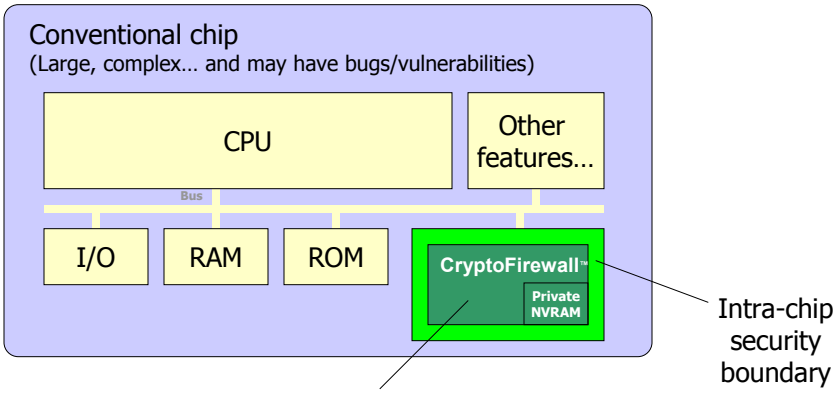
CRYPTOGRAPHY RESEARCH

RSA CONFERENCE 2007

32

CRYPTOGRAPHY RESEARCH

A Specific Example: Architecture for Tamper Resistance



Stand-alone high-security core
- Internal algorithms, keys, countermeasures…
- Assumes the rest of the chip is hostile

Cryptography Research

RSA CONFERENCE 2007

33

Architecture Elements

- Well-defined intra-chip hardware trust boundary
  - Secure even if the CPU malicious
  - Special modes (test, personalization) protected w/ strong crypto
- Strict state management
  - Hardware state well defined, minimized
  - Cryptographic hash of state at every clock cycle of the computation
- One purpose: Address tamper resistance/security
  - Information leakage: SPA / DPA / Timing
  - Glitching: Error handling and response
  - Protocol attacks: Rigid command set in hardware; strong crypto
  - Invasive attacks / Reverse engineering: Entropic array
  - Emulation: Netlist design tools
  - All software assumed malicious (CPU only performs untrusted tasks)

Cryptography Research

RSA CONFERENCE 2007

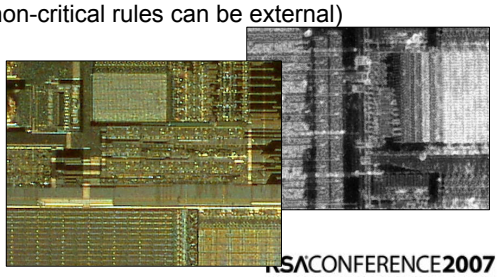
34

Cryptography Research

Special-purpose security peripherals

- Complements or replaces CPU-based enforcement mechanisms
  - Pay TV: Derivation of decryption keys
  - Mobile phones: Validation of subsidy lock
  - Payments: Security of balances & audit data
  - Printers: Authentication of consumables
  - PCs: Key management, policy enforcement, crypto

  (Support tasks and enforcement of non-critical rules can be external)



CRYPTOGRAPHY RESEARCH

RSACONFERENCE2007

35

(Background: Pay TV piracy)

- Canadians can't legally buy U.S. pay TV services
  - Willing to pay more than U.S. subscribers do (~$60/month)
  - Pirates have made a fortune breaking U.S. systems
    - Competition among pirates is fierce: attacks spread fast
    - International: Legal measures are of limited effectiveness
    - Attacks spill into the U.S. market
      - Direct losses (box subsidies) to operator
      - Indirect losses (lost revenue) content owners + operator
  - Similar dynamic elsewhere (e.g., UK expats in Germany)
- Result: Extreme pressure on the technical systems
  - Pirates willing to invest from past profits in new attacks
  - Early systems (VideoCipher II+) failed horribly

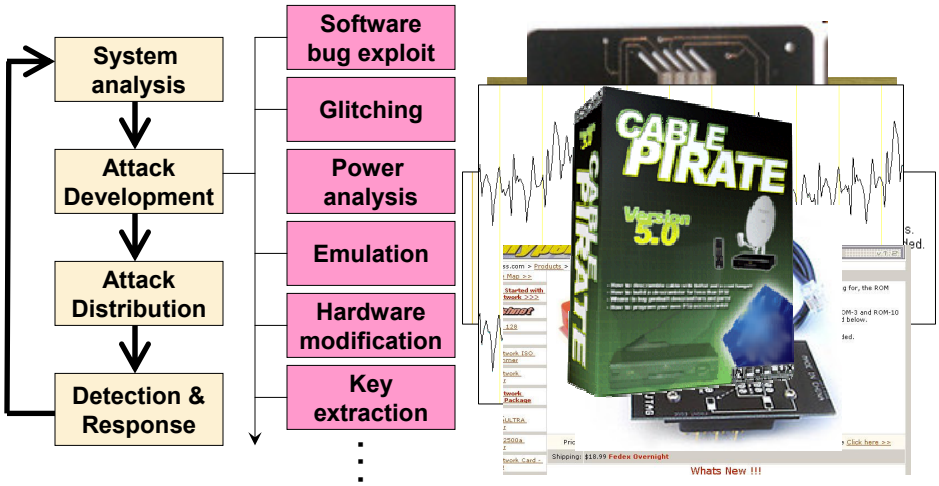
CRYPTOGRAPHY RESEARCH

RSACONFERENCE2007

36

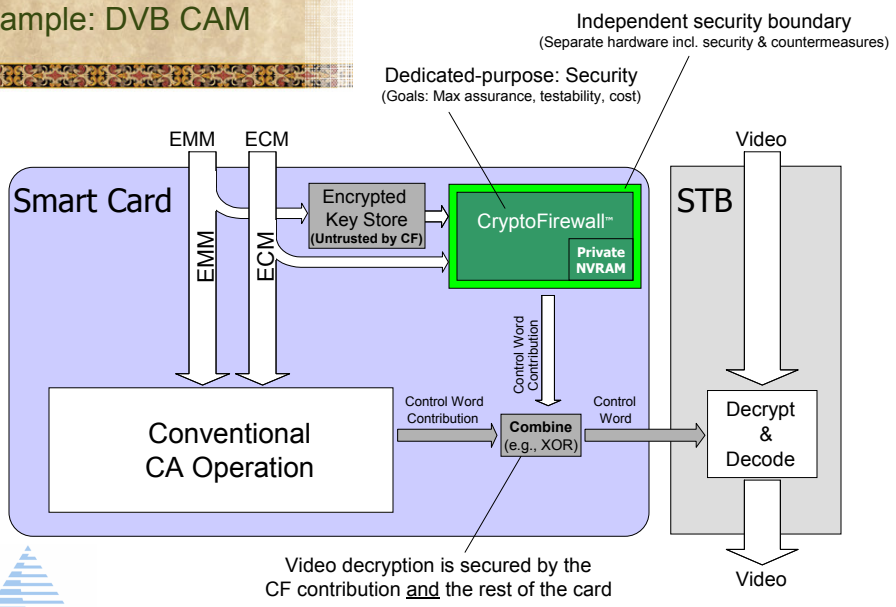
CRYPTOGRAPHY RESEARCH

Case study: Pay TV piracy



- Natural selection favors the most devastating attacks

Example: DVB CAM



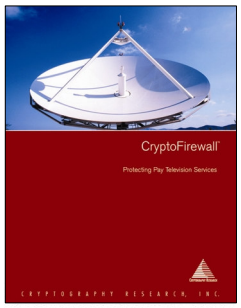
CRYPTOGRAPHY RESEARCH

RSA CONFERENCE 2007

39

Combines multiple strategies

- Hardware updates
  - Deployment part of new security module or other chip
- Security updates (patching; keys + software)
  - Piggybacked with programming data
- Redundancy-based architecture
  - Independent security elements reinforce
- So far so good:
  - Security: No news = good news…



CRYPTOGRAPHY RESEARCH

40

CRYPTOGRAPHY RESEARCH

More problems that could benefit from extra dedicated/redundant hardware

- Key management
  - Keys, passwords can be stored on separate processing engines
    - Encrypt & swap to main (untrusted) CPU as needed
- Secure input
  - Separate processing engines can handle keyboard, mouse…
- Secure display
  - Separate processing engines can control aspects of the delay (e.g., secure overlay)
- Secure storage
  - Disk encryption, file system security, etc. can also be handled separately

Cryptography Research

RSA CONFERENCE 2007

41

Caveat: Inter-related failure modes

- Problem: Failure modes be inter-related
  - Assume independence: P(fail) = P(fail1) * P(fail2)
  - Linear collapse model: T(fail) = T(fail1) + T(fail2)
  - Simultaneous collapse model: T(fail) = max(T(fail1), T(fail2))
- Case study with cryptographic secret sharing
  - CA root key stored in physical tokens
    - Goal: Avoid single modes of failure
    - After key created, audit done to verify policies
  - Key shares were in the same type of hardware
    - With the same type of battery
  - The risk was identified, but it not fixed
    - The master key was nearly lost due to battery failures

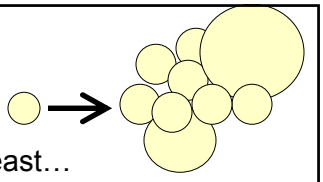
Cryptography Research

RSA CONFERENCE 2007

42

Cryptography Research

A more general approach: Micro CPUs



- A better way to invest the Moore's Law feast…
  - Add independent isolated execution areas
    - Computing areas are a resource for applications & OSes
    - Taking the "cell" microprocessor philosophy to the next level
  - Completely independent hardware
    - Separate processing capabilities
    - Separate internal RAM (even a few KB can be very useful)
    - Separate key management
    - Fully independent operation (e.g., no timing dependencies)
  - Communicates with the main CPU
    - Main CPU can perform support tasks (e.g., paging)
    - Software running on each micro-CPU should assume that the main CPU and its siblings are malicious

CRYPTOGRAPHY RESEARCH

RSA CONFERENCE 2007

43

Example: Network security

- The main CPU should not be responsible for network security
  - Too complex – numerous applications, configuration settings, drivers… A single bad ring 0 driver and it all falls down
  - … But users won't lug physical firewalls everywhere
- Solution:
  - Add a separate processing engine for firewall/VPN functionality
  - Sits between the main CPU and the network ports
    - The main CPU can't receive or transmit unauthorized data

CRYPTOGRAPHY RESEARCH

RSA CONFERENCE 2007

44

CRYPTOGRAPHY RESEARCH

Network security

- Look forward 10 years:
  - If Moore's Law continues, we'll have 1000 times as much computing hardware in 15 years…
  - We could have dozens of independent processing engines for network security – 1% would be enough for security
    - Each could handle different network security tasks (e.g., firewalling, decryption, etc.)
  - Example: Run many VPNs all at once
    - Data would pass from one to the next…
    - Use products from multiple security vendors…
    - **Add more code & security improves!**

CRYPTOGRAPHY RESEARCH

RSACONFERENCE2007

45

Conclusion;

- Future of security depends on our ability to cope with complexity
  - Patching strategies are grisly, but better than total collapse
  - But this doesn't lead to trustworthy systems…
- Hope in the gloom:
  - Use complexity to add depth and resiliency
  - Layers can fail but the system survives

CRYPTOGRAPHY RESEARCH

RSACONFERENCE2007

46

CRYPTOGRAPHY RESEARCH

Questions?…

Paul Kocher
paul@cryptography.com

Cryptography Research, Inc.
575 Market St., 21st Floor
San Francisco, CA 94105 USA

www.cryptography.com

Tel: +1 (415) 397-0123
Fax: +1 (415) 397-0127

We're hiring…

Interested in the intersection of major real-world security problems and research?

Ask me, or send e-mail to jobs@cryptography.com.

RSA CONFERENCE 2007

47