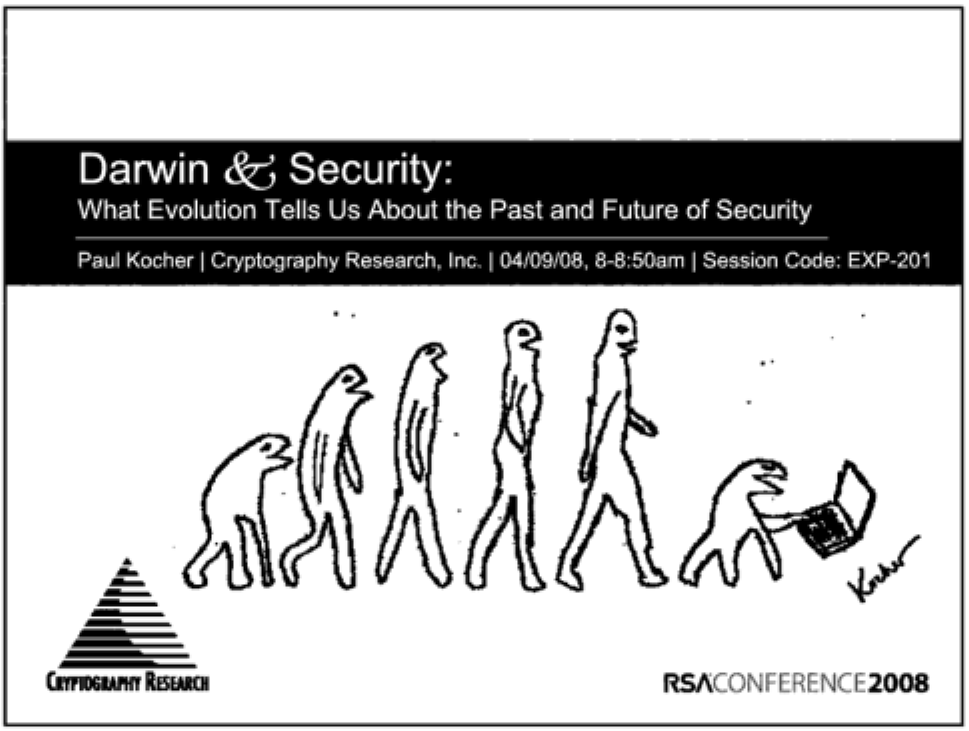


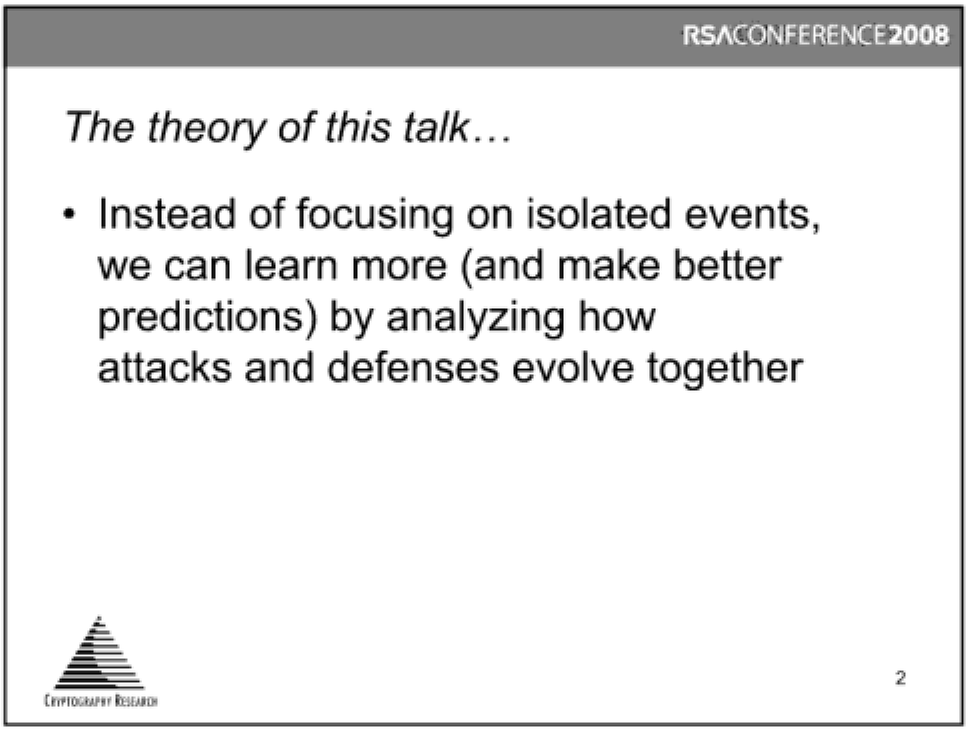
Darwin & Security:

What Evolution Tells Us About the Past and Future of Security

Paul Kocher | Cryptography Research, Inc. | 04/09/08, 8-8:50am | Session Code: EXP-201

CRYPTOGRAPHY RESEARCH

RSA CONFERENCE 2008



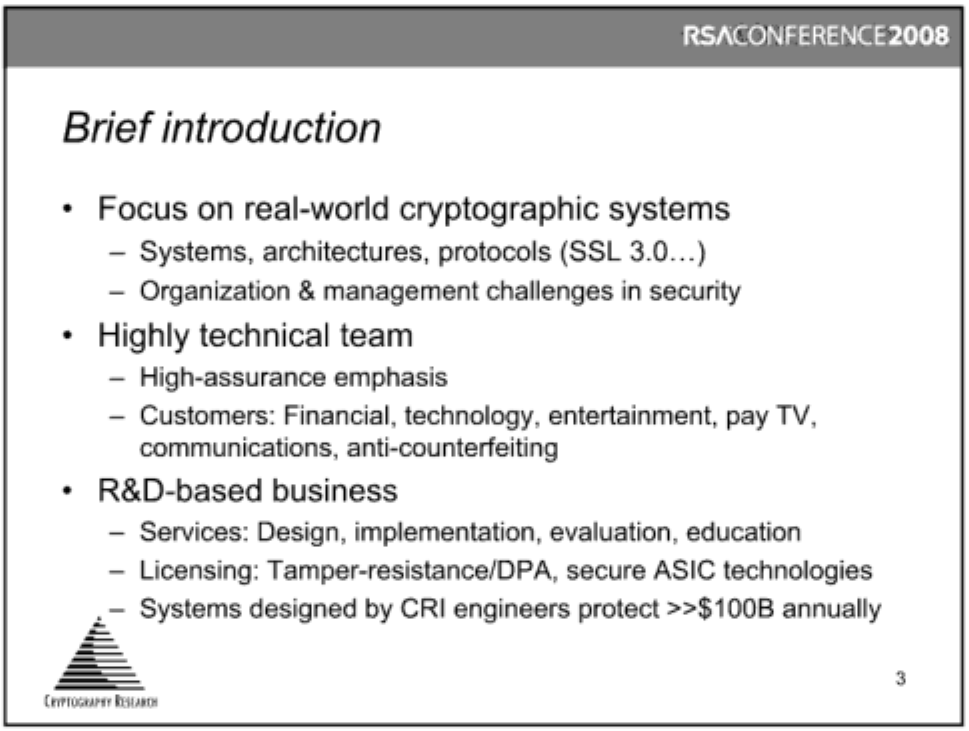
RSA CONFERENCE 2008

The theory of this talk…

- Instead of focusing on isolated events, we can learn more (and make better predictions) by analyzing how attacks and defenses evolve together

CRYPTOGRAPHY RESEARCH

2



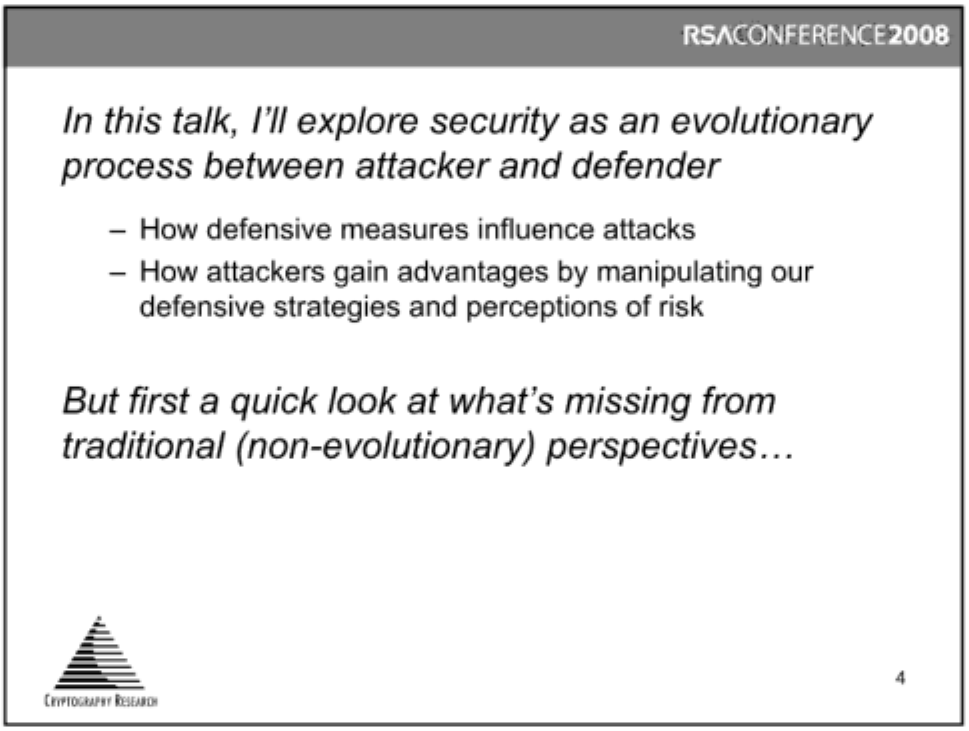
RSA CONFERENCE 2008

Brief introduction

- Focus on real-world cryptographic systems
  - Systems, architectures, protocols (SSL 3.0…)
  - Organization & management challenges in security
- Highly technical team
  - High-assurance emphasis
  - Customers: Financial, technology, entertainment, pay TV, communications, anti-counterfeiting
- R&D-based business
  - Services: Design, implementation, evaluation, education
  - Licensing: Tamper-resistance/DPA, secure ASIC technologies
  - Systems designed by CRI engineers protect >>$100B annually

CRYPTOGRAPHY RESEARCH

3



RSA CONFERENCE 2008

In this talk, I'll explore security as an evolutionary process between attacker and defender

- How defensive measures influence attacks
- How attackers gain advantages by manipulating our defensive strategies and perceptions of risk

But first a quick look at what's missing from traditional (non-evolutionary) perspectives…

CRYPTOGRAPHY RESEARCH

4

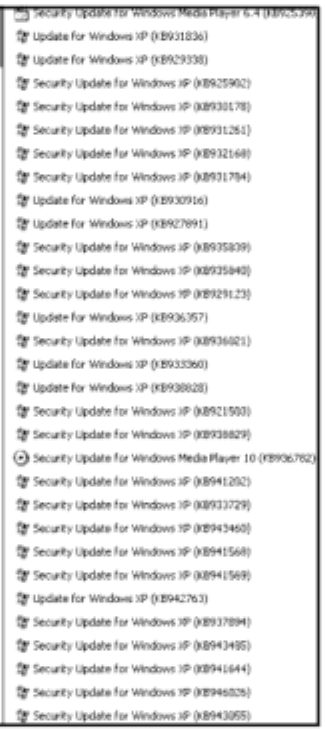
Traditional security emphasis: -- Vulnerabilities --

- Evaluations = checking for vulnerabilities
- Attacking = exploiting vulnerabilities
- Responding = patching vulnerabilities
- Engineering = introducing vulnerabilities ☺

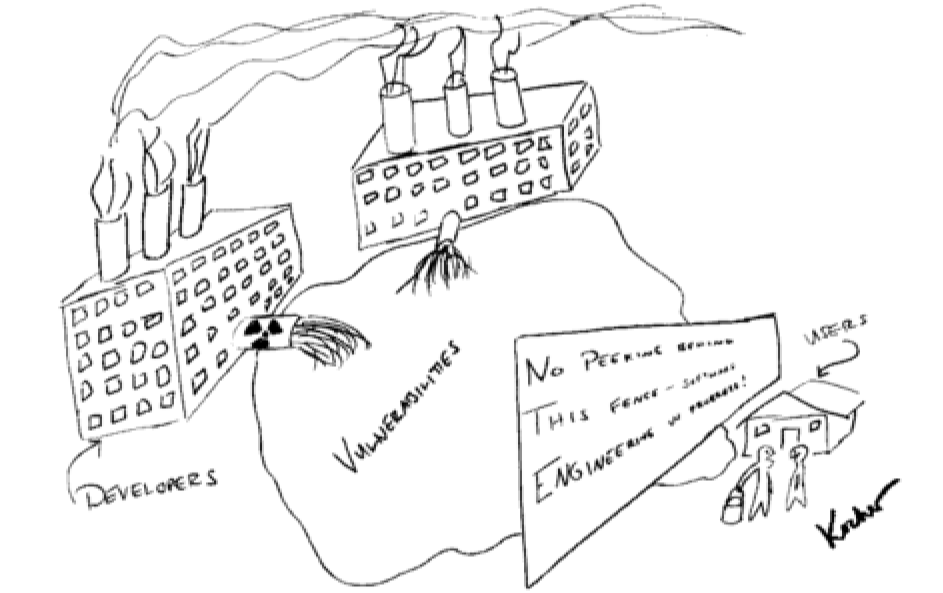
- It's all very tidy
  - Defenders have nice lists of fixed flaws
  - It appears that progress being made…

    ... but if this was working, the attackers would be giving up – which isn't happening …

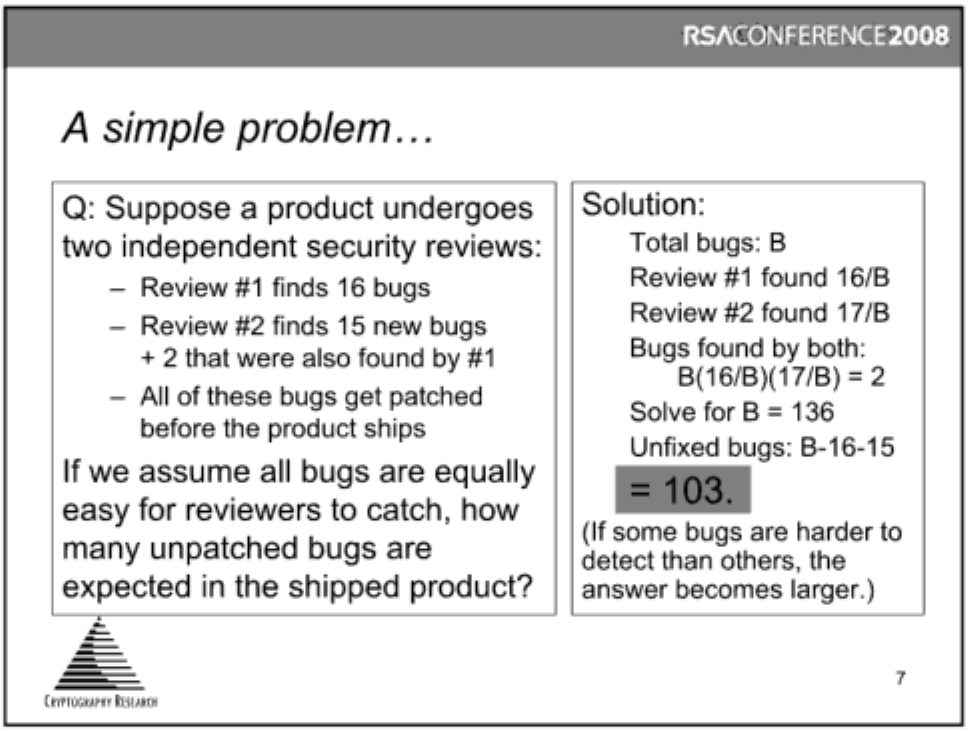
CRYPTOGRAPHY RESEARCH



Security Update for Windows Media Player 6.4 (KB92539
Update for Windows XP (KB931836)
Update for Windows XP (KB929338)
Security Update for Windows XP (KB925902)
Security Update for Windows XP (KB930178)
Security Update for Windows XP (KB931261)
Security Update for Windows XP (KB932168)
Security Update for Windows XP (KB931784)
Update for Windows XP (KB930916)
Update for Windows XP (KB927891)
Security Update for Windows XP (KB935839)
Security Update for Windows XP (KB935840)
Security Update for Windows XP (KB929123)
Update for Windows XP (KB936357)
Security Update for Windows XP (KB936021)
Update for Windows XP (KB933360)
Update for Windows XP (KB938828)
Security Update for Windows XP (KB921503)
Security Update for Windows XP (KB938829)
Security Update for Windows Media Player 10 (KB936782)
Security Update for Windows XP (KB941202)
Security Update for Windows XP (KB933729)
Security Update for Windows XP (KB943460)
Security Update for Windows XP (KB941568)
Security Update for Windows XP (KB941569)
Update for Windows XP (KB942763)
Security Update for Windows XP (KB937894)
Security Update for Windows XP (KB943485)
Security Update for Windows XP (KB941644)
Security Update for Windows XP (KB946026)
Security Update for Windows XP (KB943055)


VULNERABILITIES
NO PEEKING BEHIND THIS FENCE – SOFTWARE ENGINEERING IN PROGRESS!
USERS
DEVELOPERS
Kocher

"I'm making great progress -- I've cleaned up almost a dozen buckets out of your back yard!"



RSACONFERENCE2008

A simple problem…

Q: Suppose a product undergoes two independent security reviews:

- Review #1 finds 16 bugs
- Review #2 finds 15 new bugs + 2 that were also found by #1
- All of these bugs get patched before the product ships

If we assume all bugs are equally easy for reviewers to catch, how many unpatched bugs are expected in the shipped product?

Solution:

Total bugs: B

Review #1 found 16/B

Review #2 found 17/B

Bugs found by both:
B(16/B)(17/B) = 2

Solve for B = 136

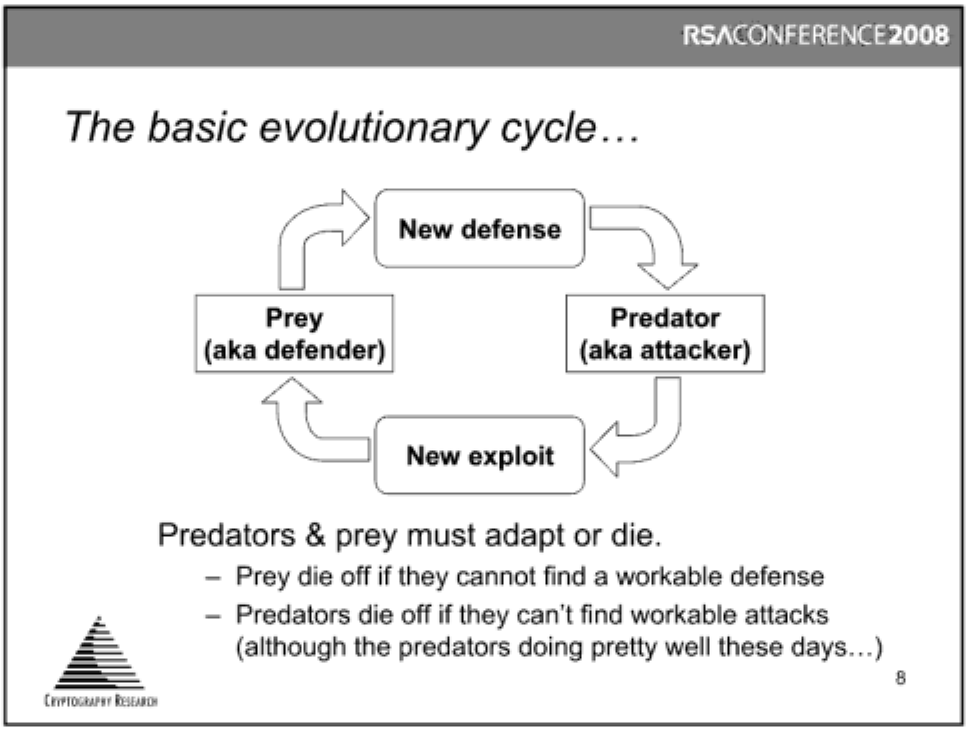
Unfixed bugs: B-16-15

= 103.

(If some bugs are harder to detect than others, the answer becomes larger.)

CRYPTOGRAPHY RESEARCH

7



RSACONFERENCE2008

The basic evolutionary cycle…

New defense

Predator
(aka attacker)

New exploit

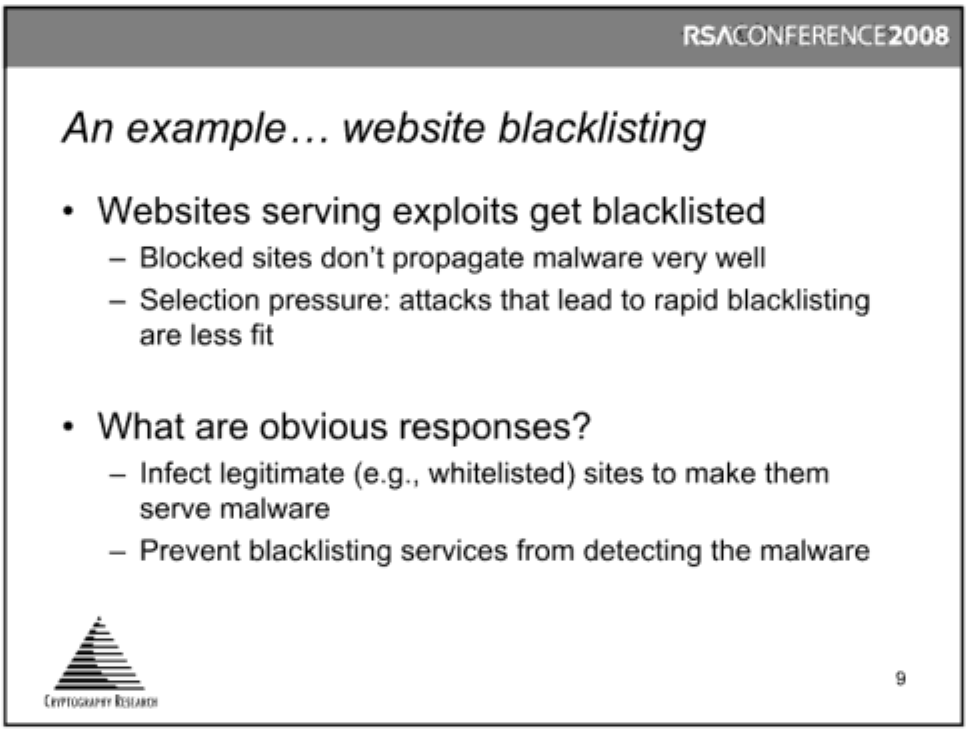
Prey
(aka defender)

Predators & prey must adapt or die.

- Prey die off if they cannot find a workable defense
- Predators die off if they can't find workable attacks (although the predators doing pretty well these days…)

CRYPTOGRAPHY RESEARCH

8



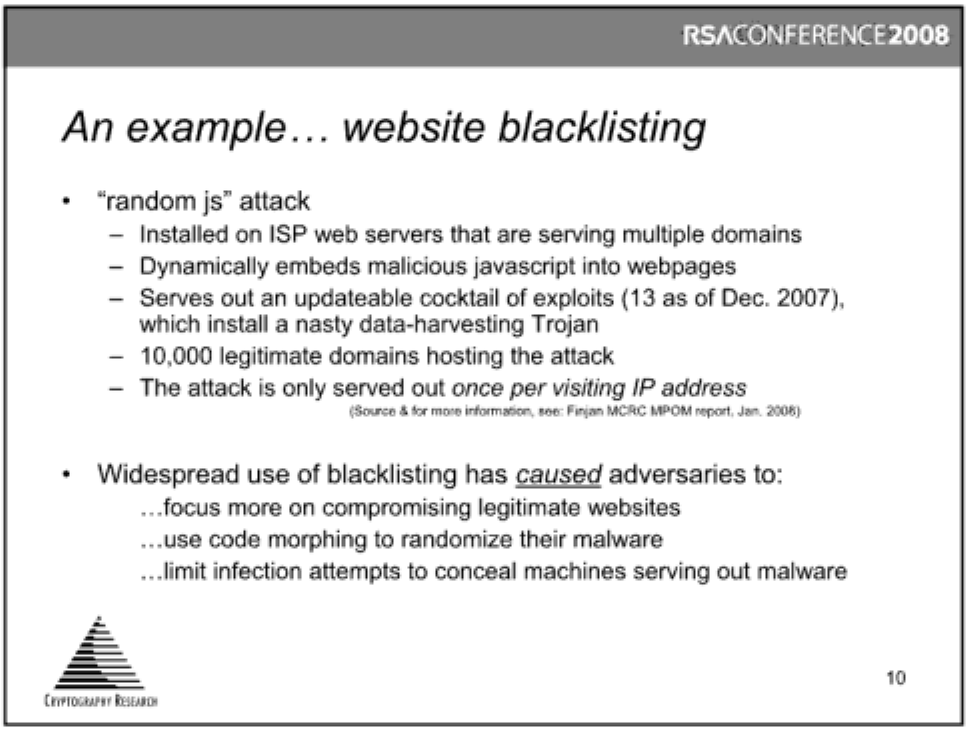
RSACONFERENCE2008

An example… website blacklisting

- Websites serving exploits get blacklisted
  - Blocked sites don't propagate malware very well
  - Selection pressure: attacks that lead to rapid blacklisting are less fit
- What are obvious responses?
  - Infect legitimate (e.g., whitelisted) sites to make them serve malware
  - Prevent blacklisting services from detecting the malware

CRYPTOGRAPHY RESEARCH

9



RSACONFERENCE2008

An example… website blacklisting

- "random js" attack
  - Installed on ISP web servers that are serving multiple domains
  - Dynamically embeds malicious javascript into webpages
  - Serves out an updateable cocktail of exploits (13 as of Dec. 2007), which install a nasty data-harvesting Trojan
  - 10,000 legitimate domains hosting the attack
  - The attack is only served out *once per visiting IP address*

(Source & for more information, see: Finjan MCRC MPOM report, Jan. 2008)

- Widespread use of blacklisting has *caused* adversaries to:

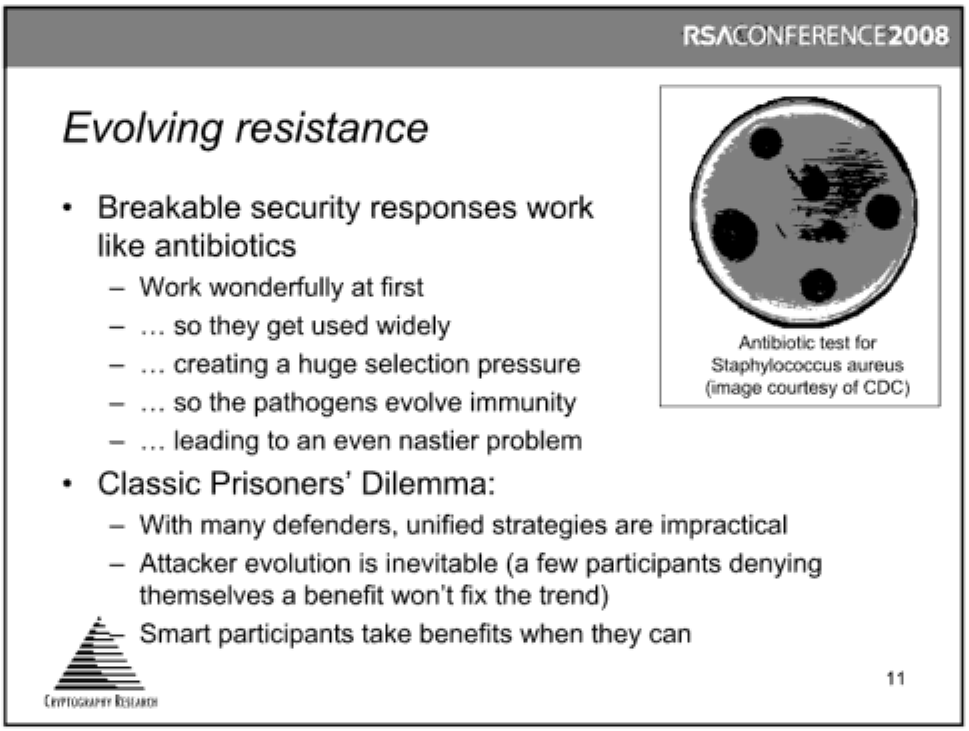
  …focus more on compromising legitimate websites

  …use code morphing to randomize their malware

  …limit infection attempts to conceal machines serving out malware

CRYPTOGRAPHY RESEARCH

10



RSACONFERENCE2008

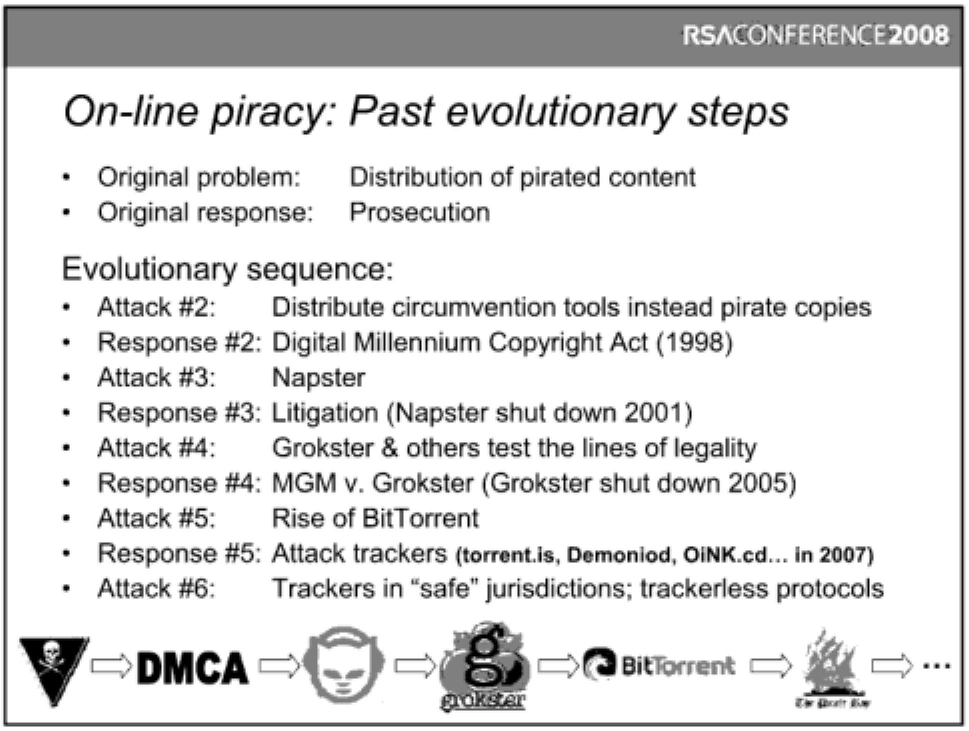
Evolving resistance

- Breakable security responses work like antibiotics
  - Work wonderfully at first
  - … so they get used widely
  - … creating a huge selection pressure
  - … so the pathogens evolve immunity
  - … leading to an even nastier problem
- Classic Prisoners' Dilemma:
  - With many defenders, unified strategies are impractical
  - Attacker evolution is inevitable (a few participants denying themselves a benefit won't fix the trend)
  - Smart participants take benefits when they can

Antibiotic test for Staphylococcus aureus (image courtesy of CDC)

CRYPTOGRAPHY RESEARCH

11



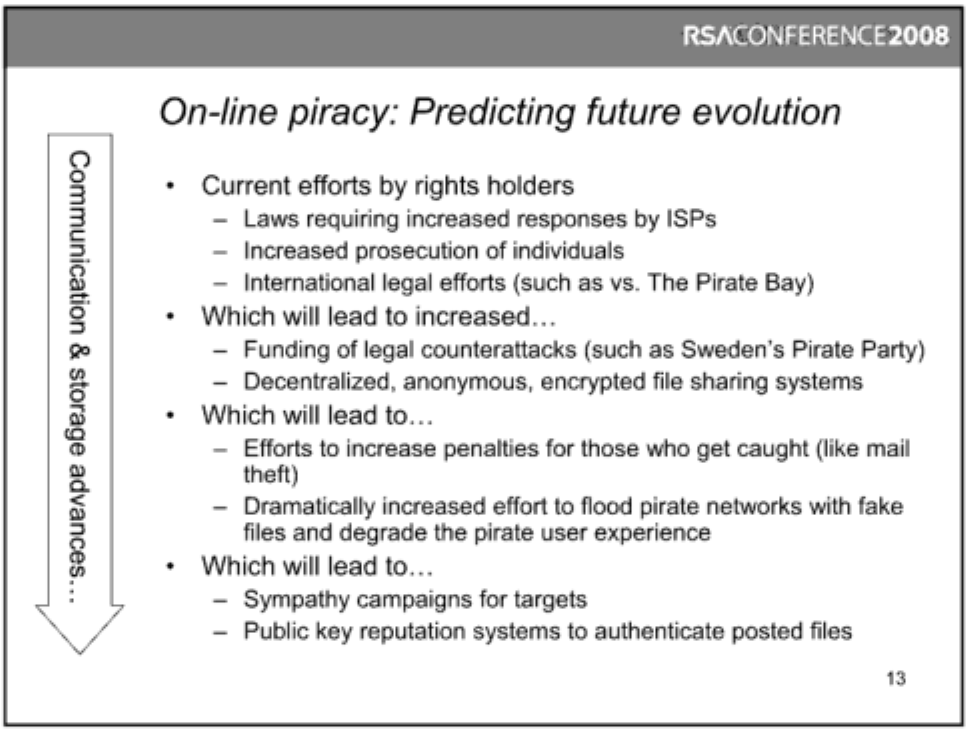
RSACONFERENCE2008

On-line piracy: Past evolutionary steps

- Original problem: Distribution of pirated content
- Original response: Prosecution

Evolutionary sequence:

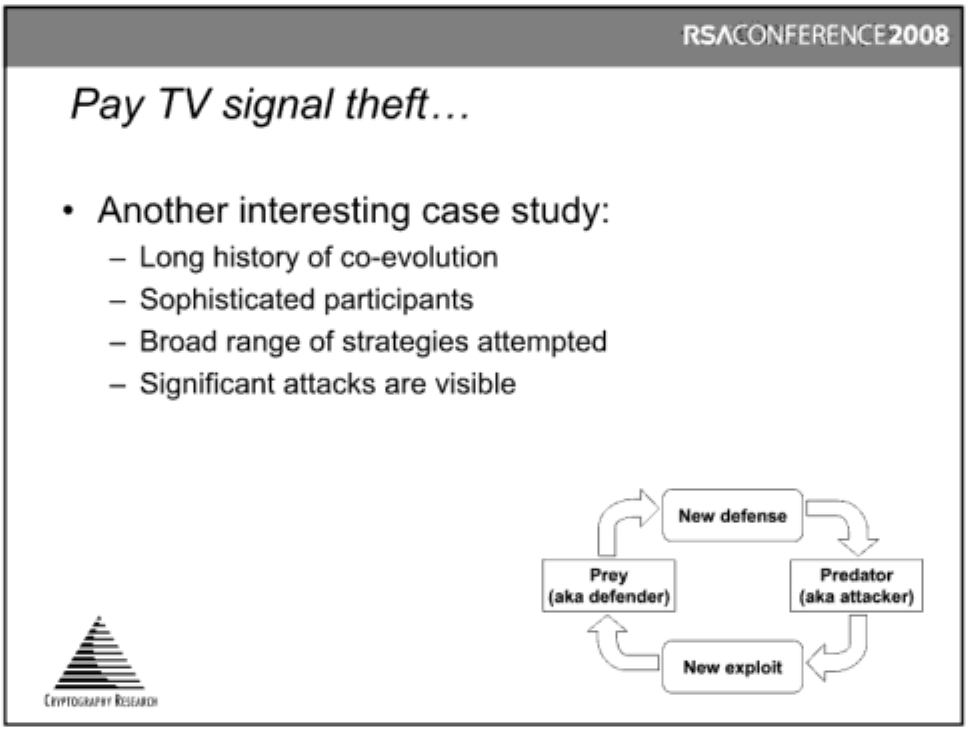
- Attack #2: Distribute circumvention tools instead pirate copies
- Response #2: Digital Millennium Copyright Act (1998)
- Attack #3: Napster
- Response #3: Litigation (Napster shut down 2001)
- Attack #4: Grokster & others test the lines of legality
- Response #4: MGM v. Grokster (Grokster shut down 2005)
- Attack #5: Rise of BitTorrent
- Response #5: Attack trackers **(torrent.is, Demoniod, OiNK.cd… in 2007)**
- Attack #6: Trackers in "safe" jurisdictions; trackerless protocols



On-line piracy: Predicting future evolution

Communication & storage advances…

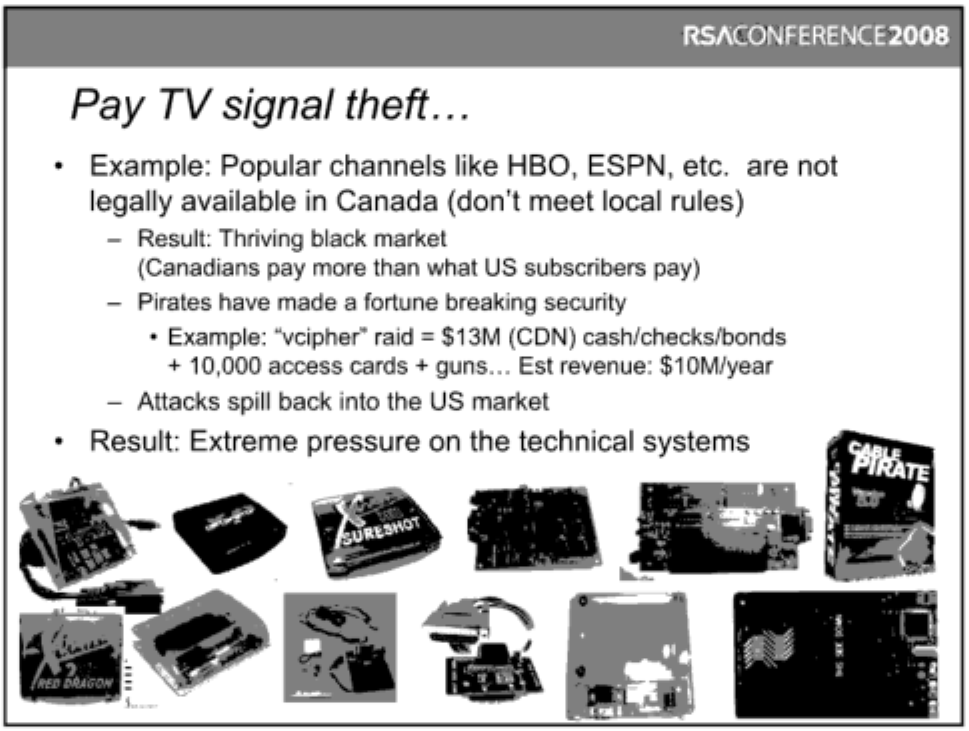
- Current efforts by rights holders
  - Laws requiring increased responses by ISPs
  - Increased prosecution of individuals
  - International legal efforts (such as vs. The Pirate Bay)
- Which will lead to increased…
  - Funding of legal counterattacks (such as Sweden's Pirate Party)
  - Decentralized, anonymous, encrypted file sharing systems
- Which will lead to…
  - Efforts to increase penalties for those who get caught (like mail theft)
  - Dramatically increased effort to flood pirate networks with fake files and degrade the pirate user experience
- Which will lead to…
  - Sympathy campaigns for targets
  - Public key reputation systems to authenticate posted files



Pay TV signal theft…

- Another interesting case study:
  - Long history of co-evolution
  - Sophisticated participants
  - Broad range of strategies attempted
  - Significant attacks are visible

New defense
Predator (aka attacker)
New exploit
Prey (aka defender)
Cryptography Research

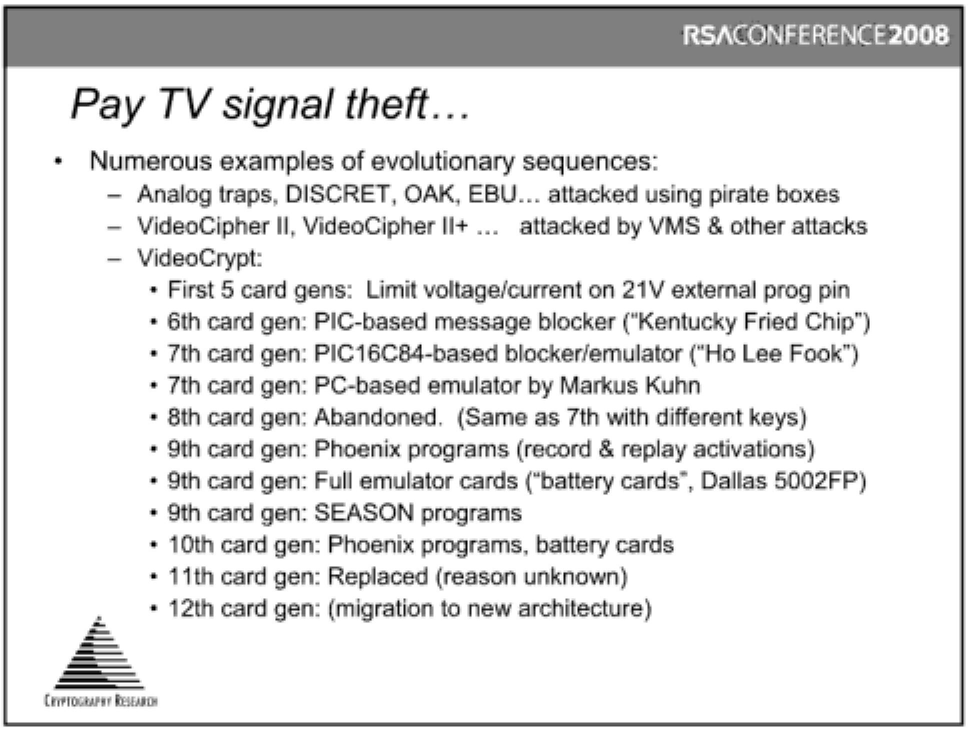


RSACONFERENCE2008

Pay TV signal theft…

- Example: Popular channels like HBO, ESPN, etc. are not legally available in Canada (don't meet local rules)
  - Result: Thriving black market
    (Canadians pay more than what US subscribers pay)
  - Pirates have made a fortune breaking security
    - Example: "vcipher" raid = $13M (CDN) cash/checks/bonds + 10,000 access cards + guns… Est revenue: $10M/year
  - Attacks spill back into the US market
- Result: Extreme pressure on the technical systems

SURESHOT
CABLE PIRATE
RED DRAGON

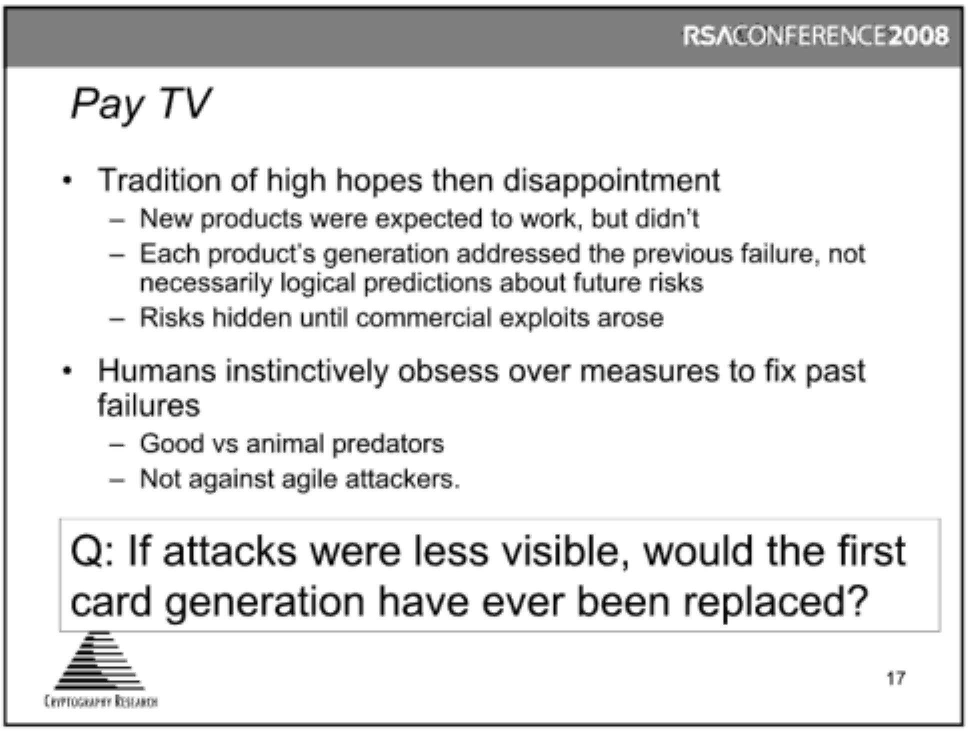


RSACONFERENCE2008

Pay TV signal theft…

- Numerous examples of evolutionary sequences:
  - Analog traps, DISCRET, OAK, EBU… attacked using pirate boxes
  - VideoCipher II, VideoCipher II+ … attacked by VMS & other attacks
  - VideoCrypt:
    - First 5 card gens: Limit voltage/current on 21V external prog pin
    - 6th card gen: PIC-based message blocker ("Kentucky Fried Chip")
    - 7th card gen: PIC16C84-based blocker/emulator ("Ho Lee Fook")
    - 7th card gen: PC-based emulator by Markus Kuhn
    - 8th card gen: Abandoned. (Same as 7th with different keys)
    - 9th card gen: Phoenix programs (record & replay activations)
    - 9th card gen: Full emulator cards ("battery cards", Dallas 5002FP)
    - 9th card gen: SEASON programs
    - 10th card gen: Phoenix programs, battery cards
    - 11th card gen: Replaced (reason unknown)
    - 12th card gen: (migration to new architecture)

CRYPTOGRAPHY RESEARCH



RSACONFERENCE2008

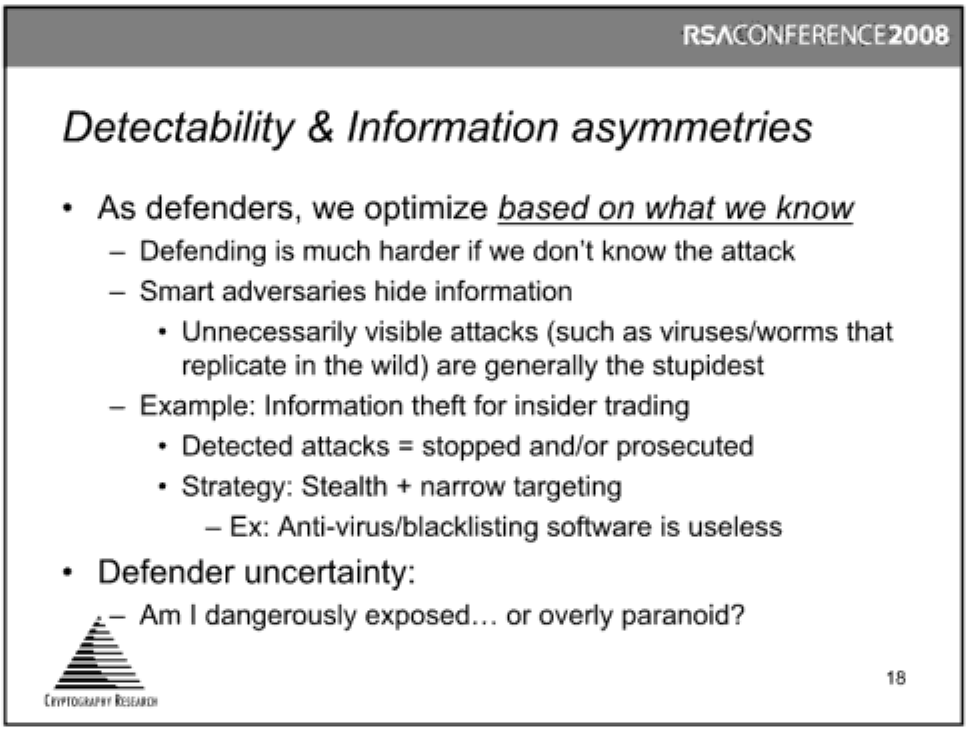
Pay TV

- Tradition of high hopes then disappointment
  - New products were expected to work, but didn't
  - Each product's generation addressed the previous failure, not necessarily logical predictions about future risks
  - Risks hidden until commercial exploits arose
- Humans instinctively obsess over measures to fix past failures
  - Good vs animal predators
  - Not against agile attackers.

Q: If attacks were less visible, would the first card generation have ever been replaced?

Cryptography Research

17



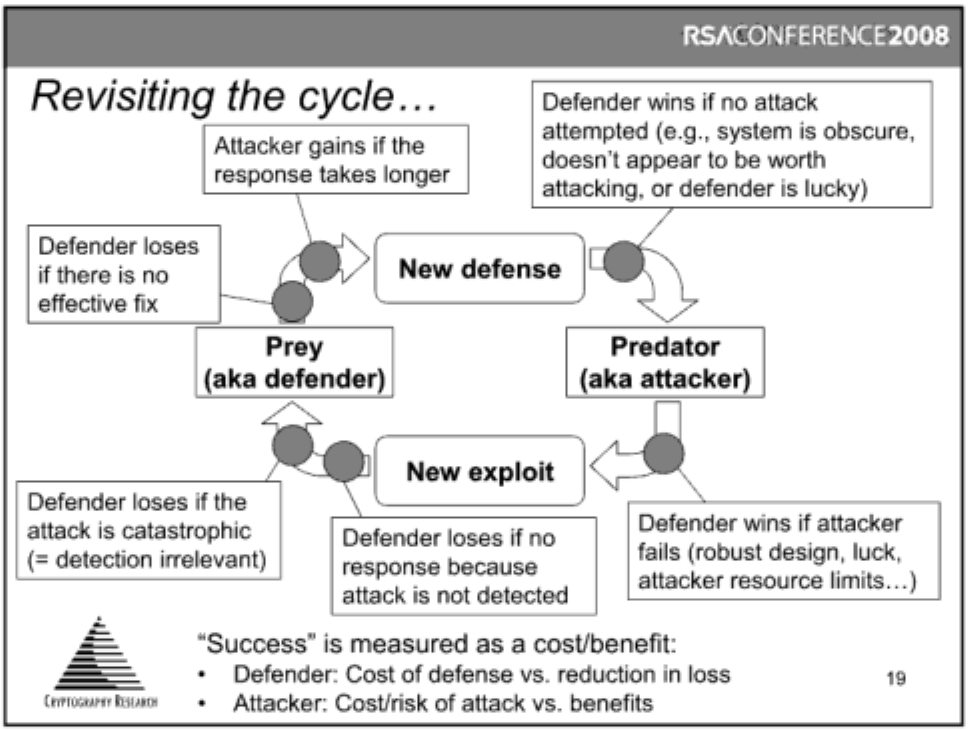
RSACONFERENCE2008

Detectability & Information asymmetries

- As defenders, we optimize *based on what we know*
  - Defending is much harder if we don't know the attack
  - Smart adversaries hide information
    - Unnecessarily visible attacks (such as viruses/worms that replicate in the wild) are generally the stupidest
  - Example: Information theft for insider trading
    - Detected attacks = stopped and/or prosecuted
    - Strategy: Stealth + narrow targeting
      - Ex: Anti-virus/blacklisting software is useless
- Defender uncertainty:
  - Am I dangerously exposed… or overly paranoid?

Cryptography Research

18

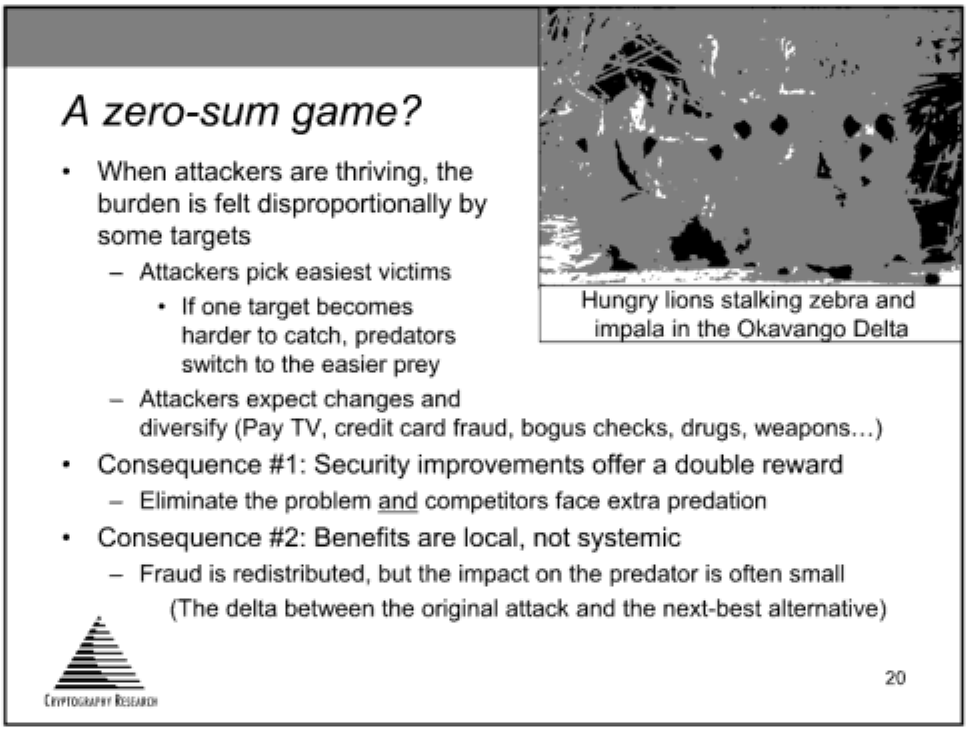


Revisiting the cycle…

Attacker gains if the response takes longer
Defender wins if no attack attempted (e.g., system is obscure, doesn't appear to be worth attacking, or defender is lucky)
Defender loses if there is no effective fix
New defense
Prey (aka defender)
Predator (aka attacker)
New exploit
Defender loses if the attack is catastrophic (= detection irrelevant)
Defender loses if no response because attack is not detected
Defender wins if attacker fails (robust design, luck, attacker resource limits…)

"Success" is measured as a cost/benefit:

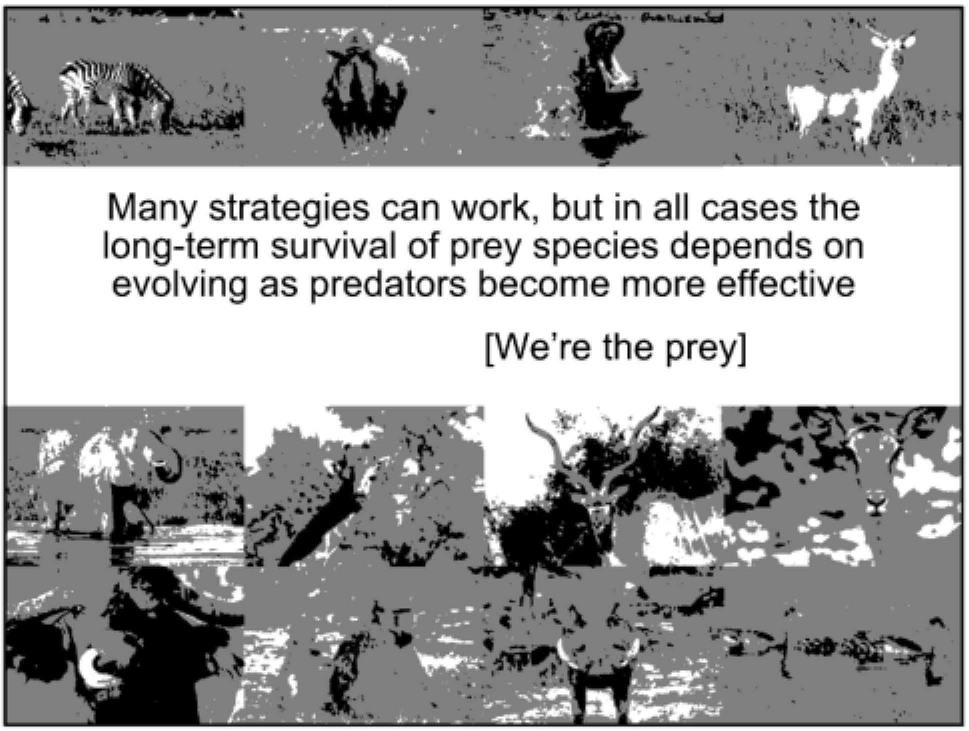
- Defender: Cost of defense vs. reduction in loss
- Attacker: Cost/risk of attack vs. benefits



A zero-sum game?

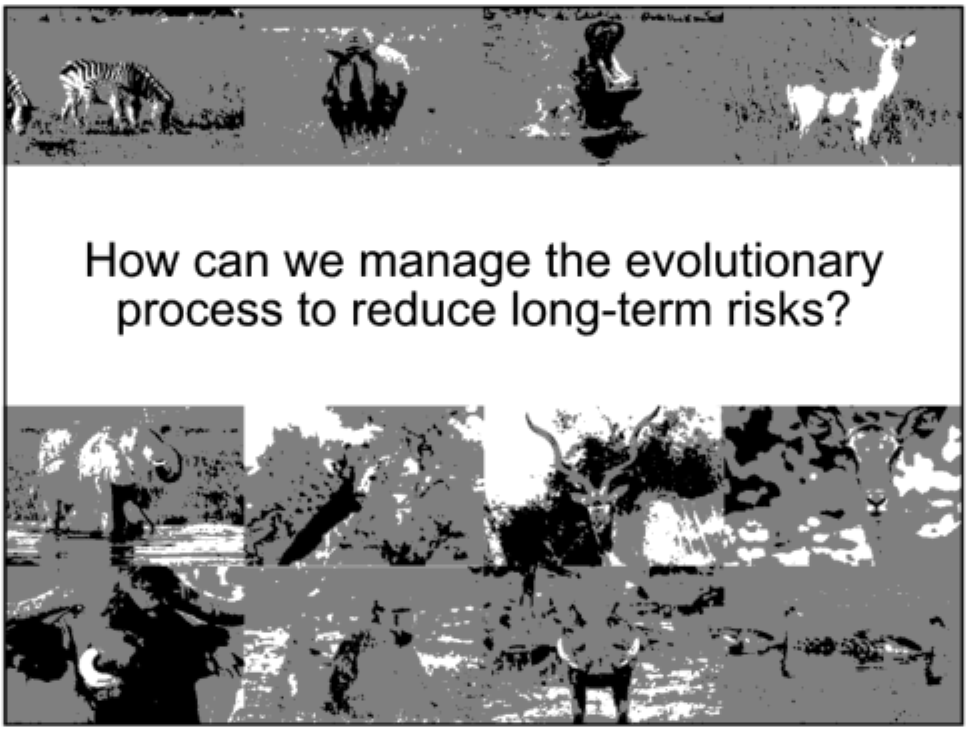
- When attackers are thriving, the burden is felt disproportionally by some targets
  - Attackers pick easiest victims
    - If one target becomes harder to catch, predators switch to the easier prey
  - Attackers expect changes and diversify (Pay TV, credit card fraud, bogus checks, drugs, weapons…)
- Consequence #1: Security improvements offer a double reward
  - Eliminate the problem and competitors face extra predation
- Consequence #2: Benefits are local, not systemic
  - Fraud is redistributed, but the impact on the predator is often small
    (The delta between the original attack and the next-best alternative)

Hungry lions stalking zebra and impala in the Okavango Delta



Many strategies can work, but in all cases the long-term survival of prey species depends on evolving as predators become more effective

[We're the prey]



How can we manage the evolutionary process to reduce long-term risks?

2006 2007 2008
VULNERABILITIES PATCHED

"If the bad guys appreciated how much effort we put into patching, do you think they might stop compromising our system?"

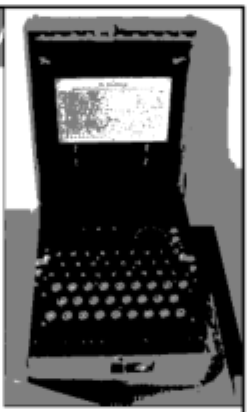
Evolving faster & better…

- Genetic improvements happen gradually
  - Less fit organisms don't propagate
- A few species specialize in a much faster way to adapt
  - Learning

Cryptography Research

Address information asymmetries that limit evolution

CRYPTOGRAPHY RESEARCH

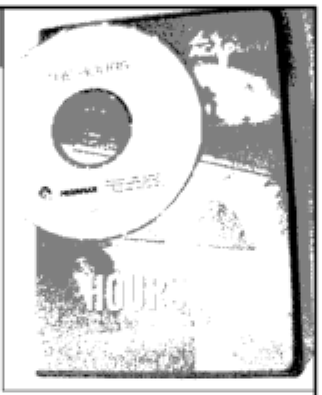


Attackers hide information to prevent good strategic decisions

- Many examples
  - Britain & US lives sacrificed to keep Germany from knowing the Enigma was broken
- But adversaries often leave hints…
  - Germans knew U-boat losses were inexplicably high, but had too much faith in the Enigma
  - Is card use at certain merchants linked to subsequent fraud?
  - Is stock trading correlated to pending M&A announcements?
  - Are solicitations from customers being sent to addresses in your mailing list?

(Tricky to distinguish clever inferences from stolen info!)

CRYPTOGRAPHY RESEARCH

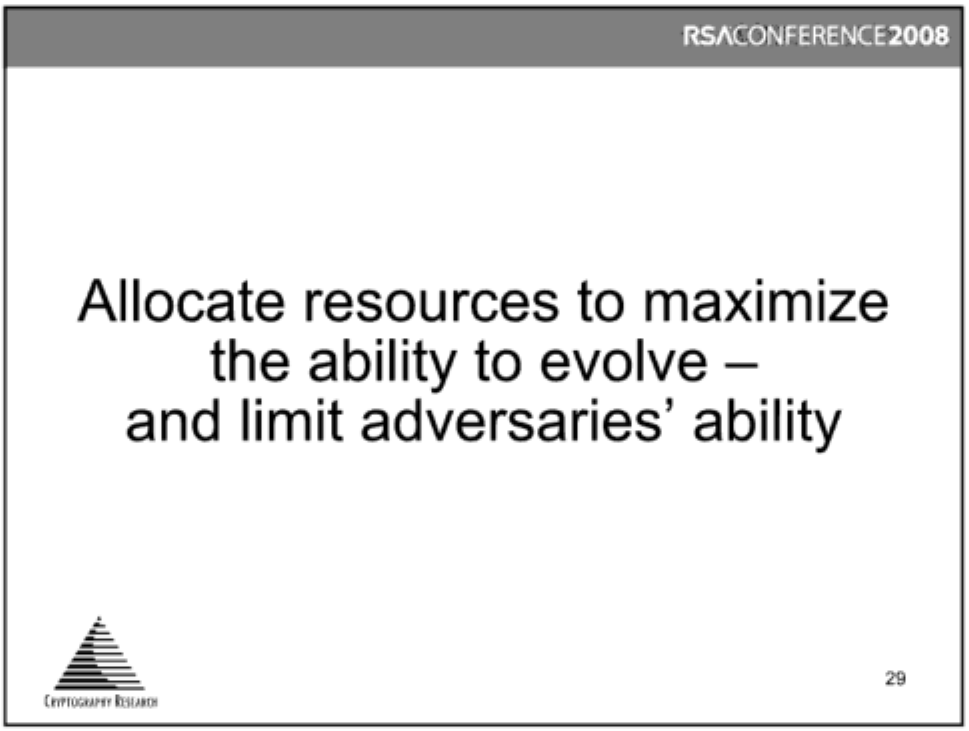


Example #1: Academy screeners…

- Academy members need to see movies so they can vote for them
  - Problem: Rampant piracy of screeners
  - Too expensive & difficult to make uncopyable
- Solution: Forensic marking
  - Unique identifying marks in each original
  - Enables copies to be traced to the Academy member
- Extra information forced the predators into the open
  - Today, movies still get pirated, but the sources get shut off quickly (+ prosecuted if appropriate, e.g. Russell Sprague)
  - Successful: Piracy from Academy screeners is now self-limiting

Example #2: Honeypots, etc.

- Problem: How to tell if outside attackers have breached a network
  - Approach: Put a honeypot on the network that will tempt adversaries who have breached the perimeter & alert you
    - If it is raided: proof something is horribly wrong
    - Useful datapoint (though not conclusive) if not breached
- Related approaches for other problems, e.g.:
  - Tempting URL in comments in sensitive source code
  - Traceable addresses in mailing list copies

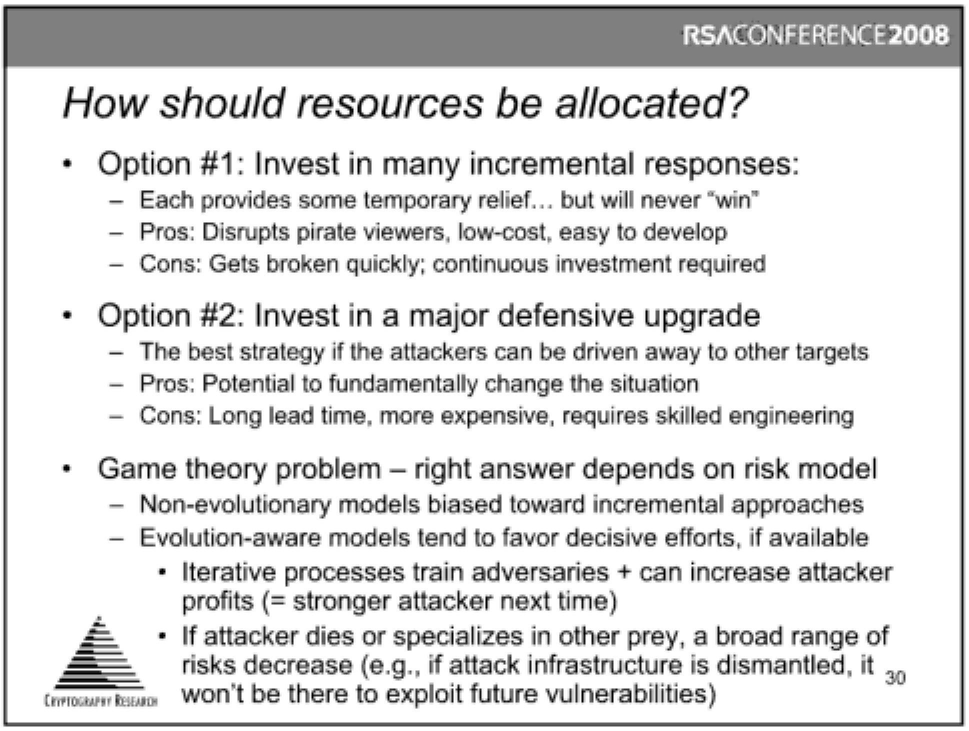


RSA CONFERENCE 2008

Allocate resources to maximize the ability to evolve – and limit adversaries' ability

Cryptography Research

29



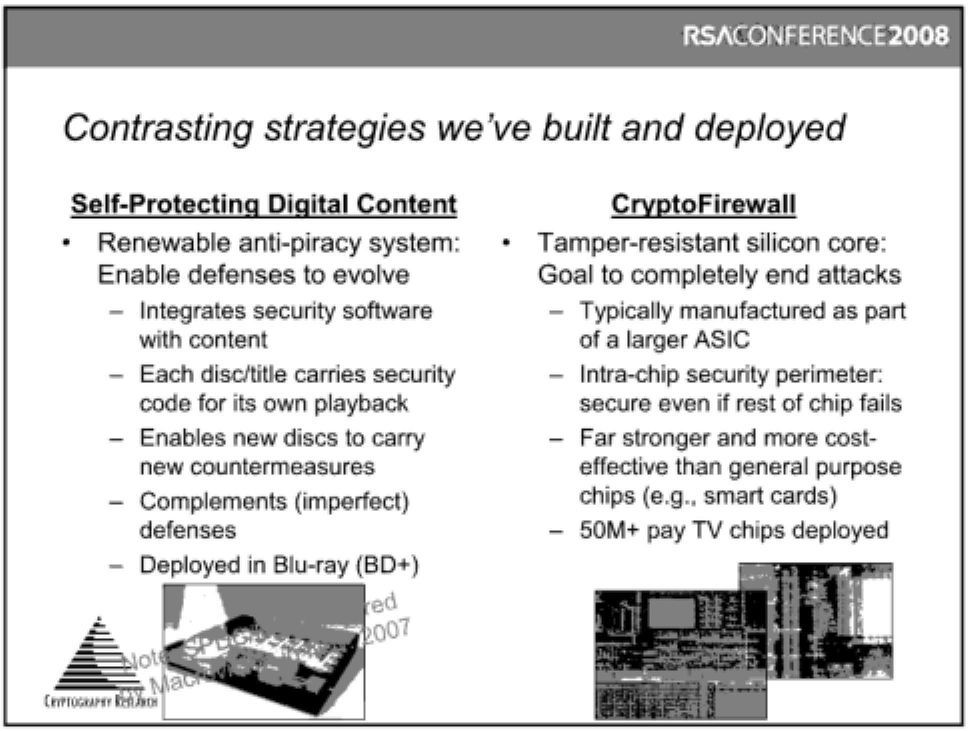
RSA CONFERENCE 2008

How should resources be allocated?

- Option #1: Invest in many incremental responses:
  - Each provides some temporary relief… but will never "win"
  - Pros: Disrupts pirate viewers, low-cost, easy to develop
  - Cons: Gets broken quickly; continuous investment required
- Option #2: Invest in a major defensive upgrade
  - The best strategy if the attackers can be driven away to other targets
  - Pros: Potential to fundamentally change the situation
  - Cons: Long lead time, more expensive, requires skilled engineering
- Game theory problem – right answer depends on risk model
  - Non-evolutionary models biased toward incremental approaches
  - Evolution-aware models tend to favor decisive efforts, if available
    - Iterative processes train adversaries + can increase attacker profits (= stronger attacker next time)
    - If attacker dies or specializes in other prey, a broad range of risks decrease (e.g., if attack infrastructure is dismantled, it won't be there to exploit future vulnerabilities)

Cryptography Research

30



RSACONFERENCE2008

Contrasting strategies we've built and deployed

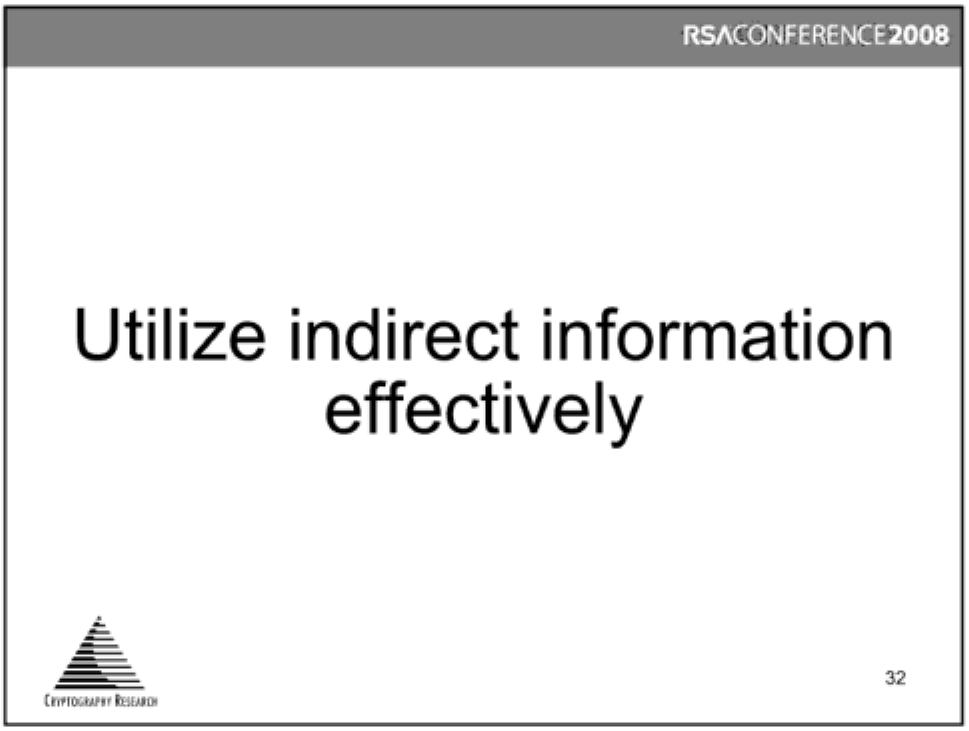
Self-Protecting Digital Content

- Renewable anti-piracy system: Enable defenses to evolve
  - Integrates security software with content
  - Each disc/title carries security code for its own playback
  - Enables new discs to carry new countermeasures
  - Complements (imperfect) defenses
  - Deployed in Blu-ray (BD+)

CryptoFirewall

- Tamper-resistant silicon core: Goal to completely end attacks
  - Typically manufactured as part of a larger ASIC
  - Intra-chip security perimeter: secure even if rest of chip fails
  - Far stronger and more cost-effective than general purpose chips (e.g., smart cards)
  - 50M+ pay TV chips deployed

CRYPTOGRAPHY RESEARCH

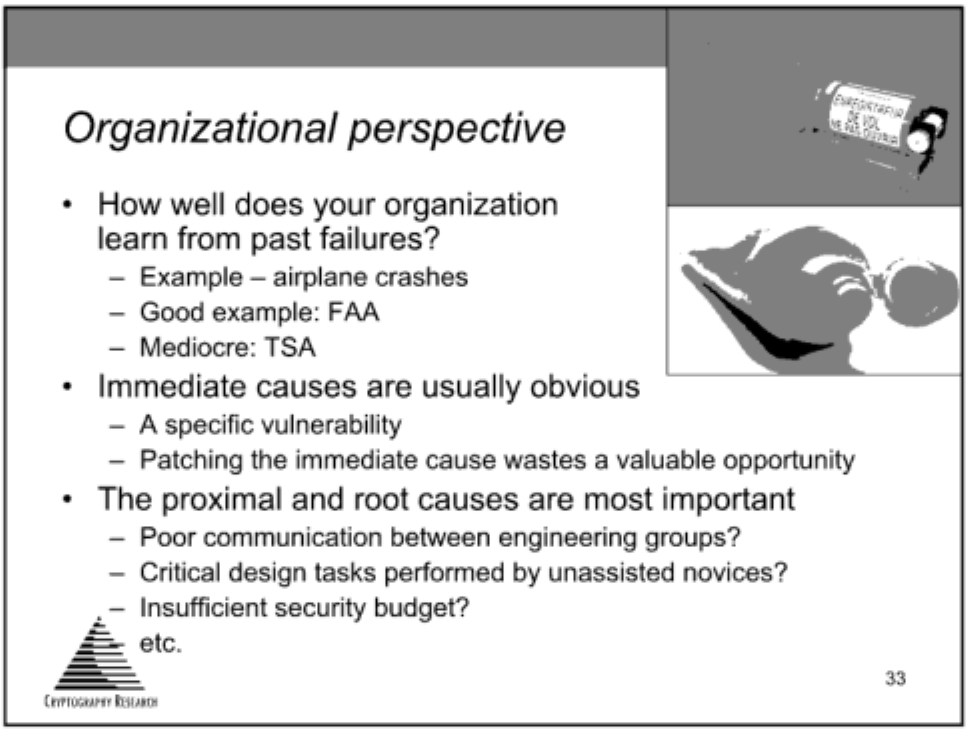


RSACONFERENCE2008

Utilize indirect information effectively

CRYPTOGRAPHY RESEARCH

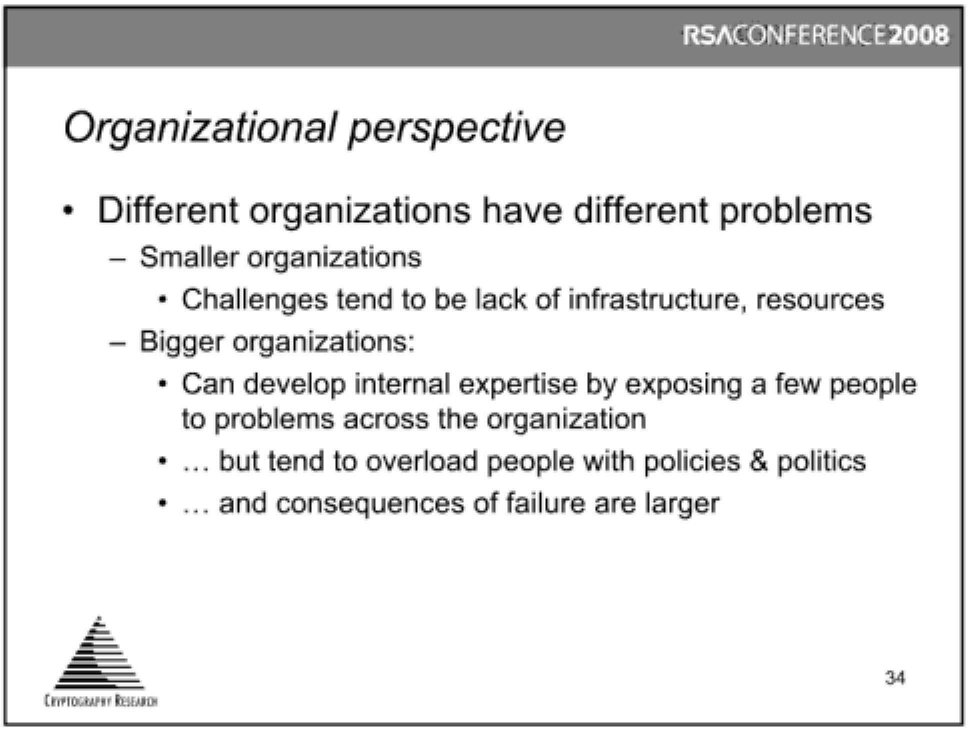
32



Organizational perspective

- How well does your organization learn from past failures?
  - Example – airplane crashes
  - Good example: FAA
  - Mediocre: TSA
- Immediate causes are usually obvious
  - A specific vulnerability
  - Patching the immediate cause wastes a valuable opportunity
- The proximal and root causes are most important
  - Poor communication between engineering groups?
  - Critical design tasks performed by unassisted novices?
  - Insufficient security budget?
  - etc.

Cryptography Research

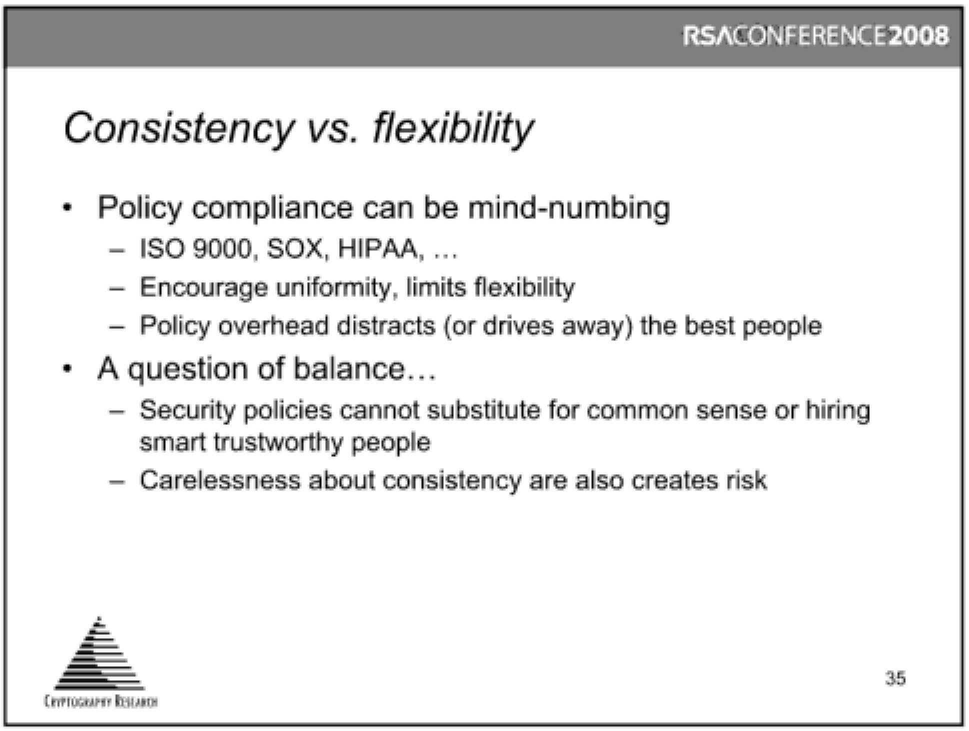


RSACONFERENCE2008

Organizational perspective

- Different organizations have different problems
  - Smaller organizations
    - Challenges tend to be lack of infrastructure, resources
  - Bigger organizations:
    - Can develop internal expertise by exposing a few people to problems across the organization
    - … but tend to overload people with policies & politics
    - … and consequences of failure are larger

Cryptography Research



Consistency vs. flexibility

- Policy compliance can be mind-numbing
  - ISO 9000, SOX, HIPAA, …
  - Encourage uniformity, limits flexibility
  - Policy overhead distracts (or drives away) the best people
- A question of balance…
  - Security policies cannot substitute for common sense or hiring smart trustworthy people
  - Carelessness about consistency are also creates risk

Cryptography Research

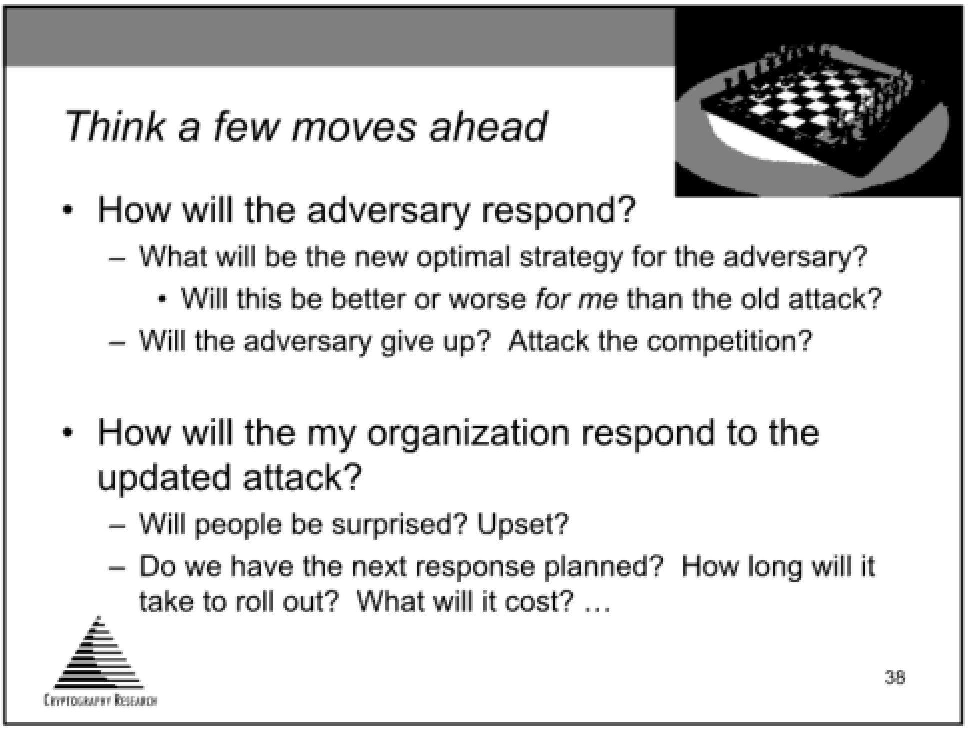
"Look at the bright side. The total network meltdown will free the IT department to focus on our core mission: audit paperwork."

RSA CONFERENCE 2008

Put yourself in the adversary's shoes

CRYPTOGRAPHY RESEARCH

37

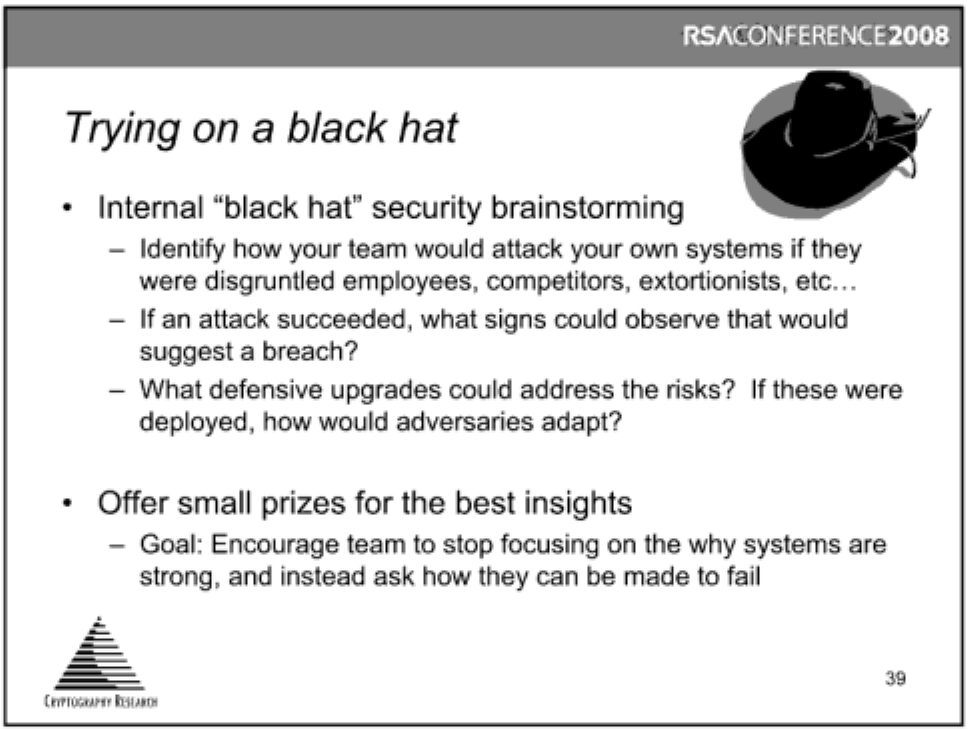


Think a few moves ahead

- How will the adversary respond?
  - What will be the new optimal strategy for the adversary?
    - Will this be better or worse *for me* than the old attack?
  - Will the adversary give up? Attack the competition?
- How will the my organization respond to the updated attack?
  - Will people be surprised? Upset?
  - Do we have the next response planned? How long will it take to roll out? What will it cost? …

CRYPTOGRAPHY RESEARCH

38



RSACONFERENCE2008

Trying on a black hat

- Internal "black hat" security brainstorming
  - Identify how your team would attack your own systems if they were disgruntled employees, competitors, extortionists, etc…
  - If an attack succeeded, what signs could observe that would suggest a breach?
  - What defensive upgrades could address the risks? If these were deployed, how would adversaries adapt?
- Offer small prizes for the best insights
  - Goal: Encourage team to stop focusing on the why systems are strong, and instead ask how they can be made to fail

Cryptography Research

39

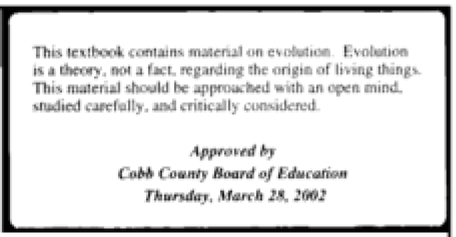
RSACONFERENCE2008

Closing thoughts

Cryptography Research

40

On "Intelligent Design"



This textbook contains material on evolution. Evolution is a theory, not a fact, regarding the origin of living things. This material should be approached with an open mind, studied carefully, and critically considered.

Approved by
Cobb County Board of Education
Thursday, March 28, 2002

- Can intelligent people build a complex system and get it right?
  - Doubtful… Windows… Linux… FreeBSD… etc.
    = too many interactions, too complex to secure reliably
- Yet we *can* build complex systems that can evolve in response to new threats
  - Windows update, SPDC…

Perhaps our best hope is to harness evolutionary processes to create systems that meet our needs…

A thought experiment on factoring…

If we want to evolve the ultimate factoring algorithm…

① Create a random algorithm

② Create some medium-sized random test integers

③ Test whether if algorithm can factor the test integers quickly

④ If not, randomly modify the algorithm and go to step 2.

⑤ Stop

Even a completely dumb process will *eventually* stumble upon the optimal factoring algorithm, but smarter approaches should yield results faster

he ultimate cryptanalytic m

a simulator that implements a basic set of

ve complex entities that study the code

When they find the answer, stop the simulation

RSACONFERENCE2008

For a copy of my slides:

Paul Kocher
paul@cryptography.com

We're hiring… Ask me or visit
www.cryptography.com/jobs

CRYPTOGRAPHY RESEARCH