"Just
because
you're paranoid
doesn't mean they
aren't out to get you."

— Anonymous (Author in hiding)

This talk is about
data security against
intelligent, motivated
bad guys.

If there is a fatal
weakness in a product…

---

Adversaries will find it
if they invest the
time and effort.

# Rational Paranoia:
# Securing Unusually High-Threat Systems

A keynote talk at the RSA 2003 Conference

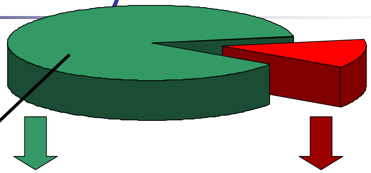
Paul Kocher

President & Chief Scientist,
Cryptography Research, Inc.

www.cryptography.com

Cryptography Research

# The Security Market



>95% of systems

System ≠ worth attacking.
Failures ≠ catastrophic.

- Off-the-shelf products work OK
  - Anti-virus software, firewalls, backup tools, scanners…
- Serious attackers won't bother.
  - Fears: Viruses, script kiddies…

Not the subject of this talk.

Facing:
Rational, determined, intelligent adversaries.

We cannot afford to learn through mistakes.

se·cu·ri·ty – (*n.*) Freedom from danger.
(Merriam-Webster Dictionary)

Assurance that bad things are unlikely to happen.

- The absence of risk.

Cryptographer's #1 fear:

- Believing security is good when it isn't.

## Strength

How strong is the system against known attacks?

Crypto can provide superb strength.

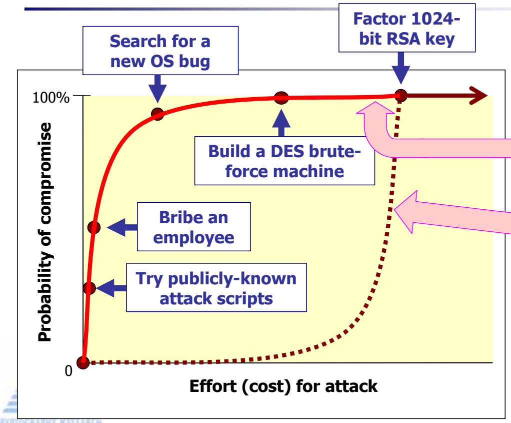
## Assurance

What are the odds of an easier (unknown) attack?

Assurance is what makes security difficult.

Getting strength or assurance is easy.
Unfortunately, we need both.

# Measuring Security



**If your curve looks like this, factoring is irrelevant.**

**You want your curve to look like this.**

**Security is NOT functionality.**

**It is the strength of the weakest link.**

# Security is not like Functionality

Most software tolerates bugs in proportion to complexity.

Example: A word processor is useful even if rarely-used functions are buggy.

Security systems are intolerant of flaws.

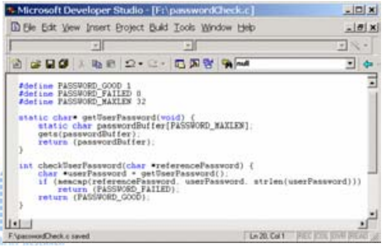
Example: A buffer overflow in rarely-used network code can be a huge security risk.

Security systems require extremely high assurance…
Yet conventional engineering is focused on functionality.

# More Complexity = Less Security

More code means:

| | |
|---|---|
| More lines of code | → More bugs |
| More interactions | → More & subtler bugs |
| Fewer testers per line | → Lower code quality |

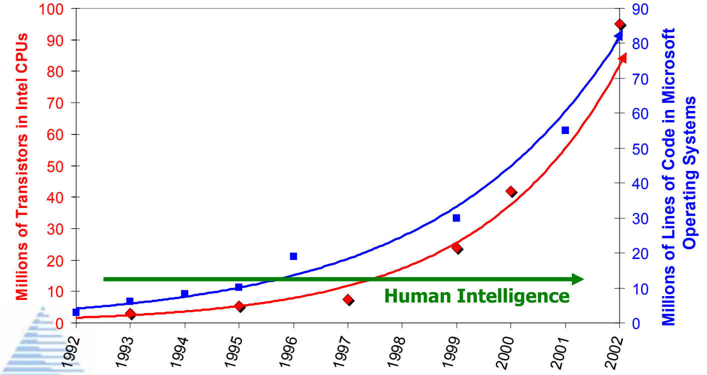

Microsoft Developer Studio - [F:\passwordCheck.c]
File Edit View Insert Project Build Tools Window Help
null
F:\passwordCheck.c saved
Ln 20, Col 1

```
#define PASSWORD_GOOD 1
#define PASSWORD_FAILED 0
#define PASSWORD_MAXLEN 32

static char* getUserPassword(void) {
    static char passwordBuffer[PASSWORD_MAXLEN];
    gets(passwordBuffer);
    return (passwordBuffer);
}

int checkUserPassword(char *referencePassword) {
    char *userPassword = getUserPassword();
    if (memcmp(referencePassword, userPassword, strlen(userPassword)))
        return (PASSWORD_FAILED);
    return (PASSWORD_GOOD);
}
```

To keep the number of flaws constant:

10X complexity → 100 to 1000X effort.

# Growth in Complexity

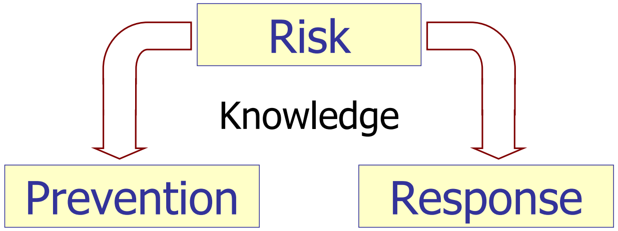


CPU data courtesy Intel Corp.

# About Cryptography Research

- Specialists in high-assurance security.
  - Highly technical.
  - Customers: Financial, technology, entertainment, pay TV, communications.
- Consulting, licensing & research.
  - Design, implementation, evaluation.
  - Licensing: Tamper-resistance/DPA, anti-piracy.
- Emphasis on solving real problems.
  - Systems designed by CRI engineers will protect >$50B in 2003.

# Living with Risk



Ex: Tamper Resistance

Ex: Controlling Piracy

A cryptographer's job should be to help understand and mitigate technology risk.

## Focus: Prevention
# Tamper Resistance

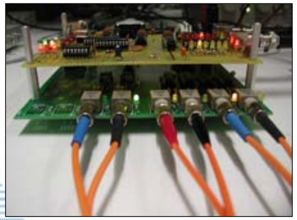
- How to protect circuits & keys against physical attack?
  - Payment cards:
    - >$1B/year fraud due to skimming.
    - Smart cards need to be secure to stop fraud growth.
  - Pay TV signal theft:
    - 5-10% fraud (Cable: $6.65B in 2000*).
  - Also for: ID cards, copy protection, counterfeit-detection…

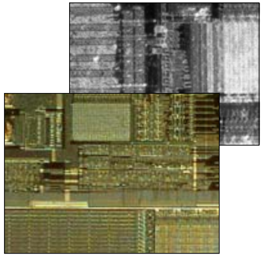
- Objectives:
  - Prevent any compromise (Prevent initial attack) AND/OR
  - Make fraud unprofitable (Prevent all easy-to-repeat attacks)

* Source: National Cable Television Association, Office of Cable Signal Theft

## Focus: Prevention
# Tamper Resistance

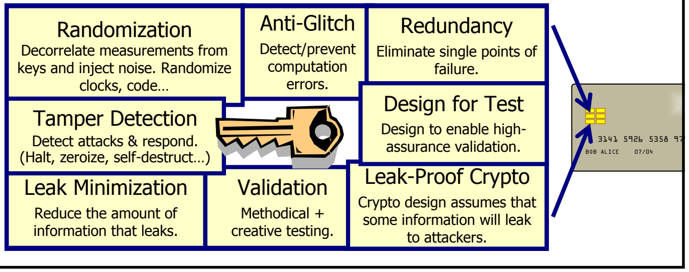
- Basic research on threats:
  - Previous industry focus: Invasive attacks, brute force/factoring.
  - Our work: Non-invasive & semi-invasive attacks
    - DPA (+EM, etc.), timing, glitching, bugs…





## Focus: Prevention
# Tamper Resistance

- Where are we today?
  - Major progress on understanding easy-to-repeat attacks.
    - The best commercial designs can be strong (but are expensive).
    - Cheaper products aren't benefiting from research.
  - Need more progress (risk is far from zero).
- Big-budget attacks remain an open problem.



Randomization
Decorrelate measurements from keys and inject noise. Randomize clocks, code…

Anti-Glitch
Detect/prevent computation errors.

Redundancy
Eliminate single points of failure.

Tamper Detection
Detect attacks & respond. (Halt, zeroize, self-destruct…)

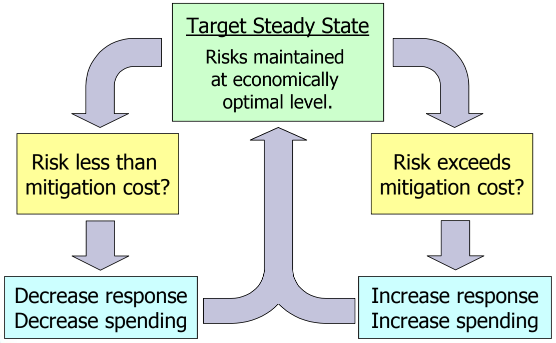
Design for Test
Design to enable high-assurance validation.

Leak Minimization
Reduce the amount of information that leaks.

Validation
Methodical + creative testing.

Leak-Proof Crypto
Crypto design assumes that some information will leak to attackers.

# Risk Management:
# When Problems are Inevitable



Target Steady State

Risks maintained at economically optimal level.

Risk less than mitigation cost?

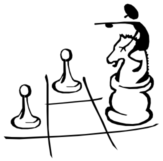
Risk exceeds mitigation cost?

Decrease response
Decrease spending

Increase response
Increase spending

# "Stalemate" Security Problems

- Last mover advantage.
  - Unpredictable, evolving threats.
    - Must present a moving target.
  - Many security problems like this:
    - Credit card fraud, SPAM filtering, piracy, virus detection.



- Research:
  Turning checkmates into stalemates:
  - Every attack must have a countermeasure.
  - Must avoid checkmate (CSS, 802.11b…).

## Focus: Recovery
# Distributing Movies on Optical Media

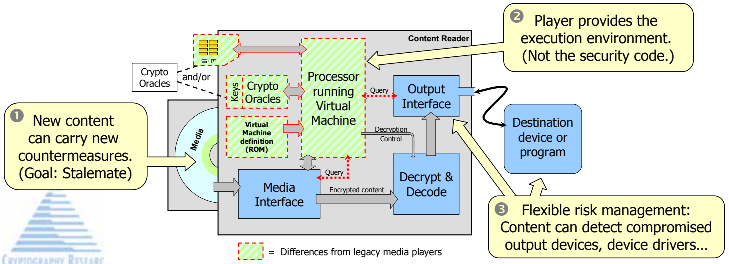
- Piracy of movies on optical media is a great example.
  - The movie industry is in trouble:
    - Moore's Law is going to make piracy much easier.
    - Alternative revenue models appear vastly inferior.
  - Piracy is an unsolvable problem:
    - Recording from analog outputs.
    - Devices will inevitably get broken.
    - No single security policy works everywhere.

The $64 ~~thousand~~ billion question:

Will piracy losses be 5% or 85% of revenue?

## Focus: Recovery
# Distributing Movies on Optical Media

- Research: Programmable security
  - Players provide a standardized execution environment.
    - Player: Virtual machine, crypto support, keys.
  - Content carries its own decoding software.
    - Total flexibility: Can have great security or no security.



❷ Player provides the execution environment. (Not the security code.)

❶ New content can carry new countermeasures. (Goal: Stalemate)

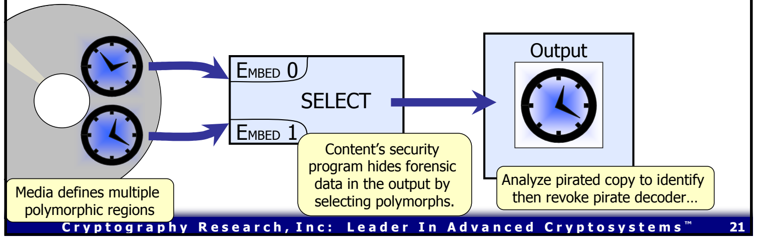
❸ Flexible risk management: Content can detect compromised output devices, device drivers…

▨ = Differences from legacy media players

## Enabling a Stalemate

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.



Media defines multiple polymorphic regions

Content's security program hides forensic data in the output by selecting polymorphs.

Analyze pirated copy to identify then revoke pirate decoder…

## The Key is Assurance

**Prevention**

Confidence that the system is robust.

**Response**

Confidence that the system isn't brittle.

http://www.nzday.com/Pages/Tairua.htm. Used w/ permission.

## The Key is Assurance

**Prevention**

Confidence that the system is robust.

**Response**

Confidence that the system isn't brittle.

- **Not a marketing message.**
- Demonstrated by:
  - A vendor's historical record
  - Objective evaluations
  - Willingness to stand behind the security (with $)

"Secure"
"Trustworthy"
"Unbreakable"
"Reliable"
"Certified"
"Hacker-Proof"
"Bulletproof"

## 10 Suggestions

❶ **View security in economic terms.**

- Assign a dollar-value to your risk.
  - Get management support for the estimate.
- Spend before problems get out of control.

Cryptography Research

## 10 Suggestions

➊ View security in economic terms.

**➋ Think about how risk is allocated.**

- Where are the single points of failure?
- Will those who control your risk share it?
- Are the people you trust actually trustworthy?
  - What is their historical track record?
  - Do they make unsubstantiated claims of "security"?
  - Who can vouch for their work?

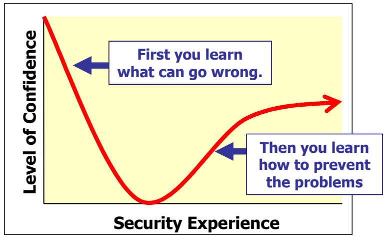
## 10 Suggestions

➊ View security in economic terms.

➋ Think about how risk is allocated.

**➌ Be humble and know your limits.**

- Don't mistake confidence for experience.
- Encourage people to look for flaws in your work.
- Don't assume attackers won't "figure it out".



## 10 Suggestions

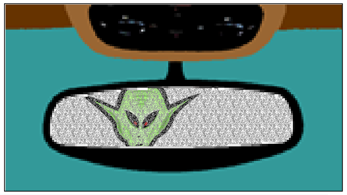
➊ View security in economic terms.

➋ Think about how risk is allocated.

➌ Be humble and know your limits.

**➍ Make realistic assumptions.**

- Assume that users are lazy and gullible.
- Assume that engineers make mistakes.
- Beware of the rear view mirror.
  - Your greatest risk may not be what went wrong last time.



## 10 Suggestions

➊ View security in economic terms.

➋ Think about how risk is allocated.

➌ Be humble and know your limits.

➍ Make realistic assumptions.

**➎ Minimize complexity.**

- Isolate critical components.
- Beware of complex interfaces.
- Have the courage to resist adding features.

Unnecessary complexity
is a <u>security flaw</u>.

## 10 Suggestions

❶ View security in economic terms.

❷ Think about how risk is allocated.

❸ Be humble and know your limits.

❹ Make realistic assumptions.

❺ Minimize complexity.

**❻ Spend more on evaluation than design.**

- Evaluations can only prove insecurity.
  - Beware of iterative testing.
- Make sure evaluators are skilled and objective.
  - Don’t impose unreasonable restrictions.
  - Requires creativity, experience, attention to detail.

## 10 Suggestions

❶ View security in economic terms.

❷ Think about how risk is allocated.

❸ Be humble and know your limits.

❹ Make realistic assumptions.

❺ Minimize complexity.

❻ Spend more on evaluation than design.

**❼ Be a skeptic.**

- Assume systems are insecure unless you have evidence to the contrary.
  - Avoid anything undocumented or untestable.
- Ask tough questions and demand responses.
  - Don’t be impressed by the line:
    “We can’t tell you for security reasons.”

## 10 Suggestions

❶ View security in economic terms.

❷ Think about how risk is allocated.

❸ Be humble and know your limits.

❹ Make realistic assumptions.

❺ Minimize complexity.

❻ Spend more on evaluation than design.

❼ Be a skeptic.

**❽ Plan for trouble.**

- What happens after a breach?
  - Will you know if there was a breach?
- Keep good audit records.
- Are “impossible” attacks really impossible?

Image courtesy NTSB.

## 10 Suggestions

❶ View security in economic terms.

❷ Think about how risk is allocated.

❸ Be humble and know your limits.

❹ Make realistic assumptions.

❺ Minimize complexity.

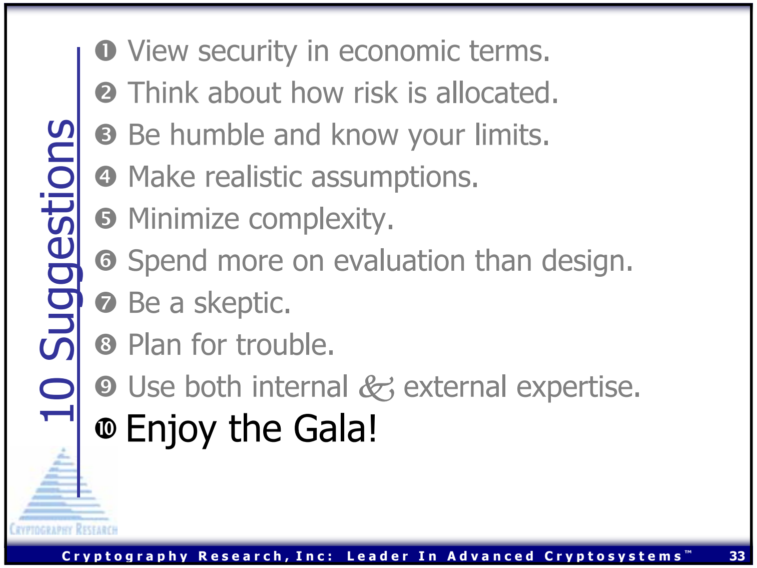
❻ Spend more on evaluation than design.

❼ Be a skeptic.

❽ Plan for trouble.

**❾ Use both internal & external expertise.**

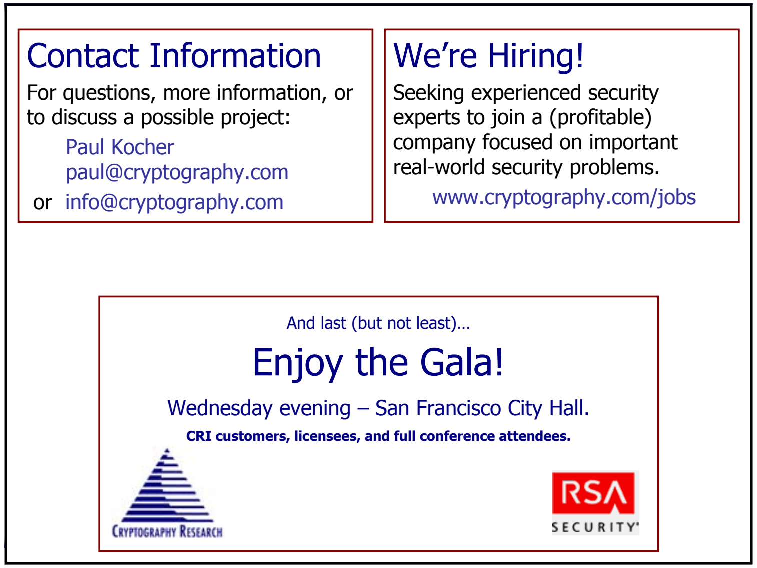
- Risks are much higher if you rely only on just one.
- Get multiple opinions, especially if you fear: piracy, fraud, espionage, or product recalls.



## 10 Suggestions

1. View security in economic terms.
2. Think about how risk is allocated.
3. Be humble and know your limits.
4. Make realistic assumptions.
5. Minimize complexity.
6. Spend more on evaluation than design.
7. Be a skeptic.
8. Plan for trouble.
9. Use both internal & external expertise.
10. **Enjoy the Gala!**

Cryptography Research



## Contact Information

For questions, more information, or to discuss a possible project:

Paul Kocher
paul@cryptography.com
or info@cryptography.com

## We're Hiring!

Seeking experienced security experts to join a (profitable) company focused on important real-world security problems.

www.cryptography.com/jobs

And last (but not least)…

## Enjoy the Gala!

Wednesday evening – San Francisco City Hall.

**CRI customers, licensees, and full conference attendees.**

Cryptography Research

RSA SECURITY®