

Ten Bugs That Cost Our Customers Billions




Benjamin Jun, VP of Technology
Cryptography Research, Inc.



RSA Conference 2005


Why a top 10?



- Commercial security is a young field (<30 yrs)
 - Still developing solid certifications and quality metrics
- Piracy and fraud follow similar, predictable patterns
 - Systems worth attacking attract well equipped attackers
- The absence of security is extremely expensive
 - Poor infrastructure wastes everyone's resources and ruins the possible
 - Wasteful engineering, mediocre product differentiation, bad security

"It's Déjà vu all over again" – Yogi Berra

RSA Conference 2005



What to look for



- Look for an underlying human “problem”
 - Over-confidence
 - Poor design or operational decision
 - Feature creep towards oblivion
- Did “comps” escape the problem?
 - Systems with similar technology and security requirements
 - Often in industries with different approach to problem-solving



“Why do you look at the speck of sawdust in your brother's eye and pay no attention to the plank in your own eye?”
— Matthew 7:3

RSA Conference 2005



Who am I? What do I do?



- Cryptography Research
 - Develop & license new security technologies
 - Provide design and evaluation services
 - Major R&D focus on solving real-world security problems
- Industries served:
 - Financial
 - Entertainment / Pay TV
 - Tamper resistance
 - Wireless / Telecommunications
 - Internet

Products incorporating CRI technology
secure over \$100B annually

RSA Conference 2005



Bug #10: DVD CSS



Crypto algorithm failure.

- DVD content protection
 - Content on disk is encrypted
- CSS algorithm
 - Inexperienced designers
 - Not adequately reviewed
- 1999: CSS broken, keys extracted
 - Johansen (& others) release DeCSS
 - Ripping software widely available



RSA Conference 2005



Bug #10: DVD CSS



Crypto algorithm failure.

- Crypto failure = no incentive for other attacks
- Knock-off (unlicensed) DVD players
- DMCA legal provisions applied with mixed results

- Bad crypto algorithms are inexcusable
 - DST RFID, CAVE, 3GPP, A5, COMP128, ... lots more!
 - There is a solid body of knowledge on crypto design
 - Seek help if you must employ proprietary designs!



RSA Conference 2005



Bug #9: Pachinko Stored Value Fraud



Stored value product cloned to “generate” funds.

- Stored value cards issued for Pachinko parlors
 - Designed to limit tax evasion, money laundering
 - Deployed in conjunction with industry, regulators, and portfolio managers
- Attackers cloned the cards
 - Cards were anonymous, high-value, redeemable for cash
 - Losses > \$600M
 - Organized crime difficult to trace, N. Korea involvement believed



The Impact of Fraud on New Methods of Retail Payment, William Roberts, Federal Reserve Bank of Atlanta, 1998;
WSJ May 22, 1996; Image courtesy Andrew, used with permission, <http://homepage.mac.com/westernrobot>

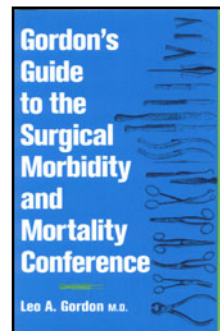


Bug #9: Pachinko Stored Value Fraud



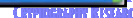
Stored value product cloned to “generate” funds.

- **\$600M!** What happened?
 - Regulators unsophisticated in associated business risks
 - Parlor operators not responsible for losses
 - Operational structure prevented bad news from traveling upstream
- Seek to risk manage “unsolvable” problems
 - Expect problems and expect to learn from them!
 - Policies should align interests of responsible parties
 - Good: Credit card merchant agreements
 - Bad: Camcording / movie theater operators



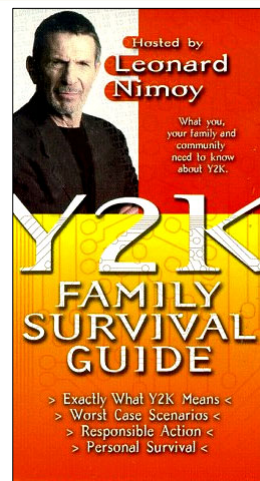
WSJ May 22, 1996

RSA Conference 2005



**Bug #8:
Y2K****Data structures matter.**

- Not a security problem...
 - Critical data fields couldn't handle rollover
 - Problems at system data junctions
 - Undocumented legacy systems
 - But repair costs staggering!
- Causes
 - "Clever" designers, data inconsistencies, and patchwork infrastructures
 - Limitations in software testability



Y2K Family Survival Guide
Monarch Home Video, 1999

RSA Conference 2005

**Bug #8:
Y2K****Data structures matter.**

- Check critical data fields for security implications
 - Data can be under-scoped or excessively complex
 - Developers have huge discretion— ask for help!
 - Feature creep is a huge challenge
- Next crisis: Security data structures
 - ID: "Computer Assisted Passenger Screening", ICAO e-passport, state drivers licenses, government ID (CAC)...
 - IT: Federated identity management, X.509, ...
 - Financial: Check 21, ...

RSA Conference 2005



Bug #7: Napster / P2P



Improved delivery mechanisms simplify content attacks.

- Peer-to-peer filesharing
 - Envisioned by AFS and other filesystems
 - Moore's law, networking infrastructure
- Napster led the pack
 - Centralized indexing, easy user experience
- "File sharing" becomes synonymous with copyright infringement
 - Majority of Napster content was illegal
 - Music sales fall



Napster Logo

RSA Conference 2005

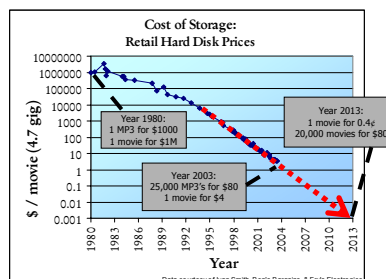


Bug #7: Napster / P2P



Improved delivery mechanisms simplify content attacks.

- Aggressive networks emerge
 - "Improved" technology
 - Decentralization, anonymity, deniability, feedback
 - Harder to shut down, harder to trace
- Next step: movies!
 - MP3 to DVD...10 yrs. of Moore's law
- Inflection point: high-definition formats
 - HD content offers new opportunities (and risks)



RSA Conference 2005

Source: Cryptography Research



Bug #7: Napster / P2P



Improved delivery mechanisms simplify content attacks.

- Look to industries that face “unsolvable problems”
 - Last mover wins: Credit card fraud, anti-Spam, anti-virus, ...

Detect

Respond

- Format upgrades should enable control of risk
 - Example: Content code directs playback on a player-based VM
 - Detection: Forensic marking capability, playback environment analysis
 - Updates: New discs contain new countermeasures

- A different mindset...
 - Goal: Extend content release window
 - Forward security: New content resistant to previous attacks

RSA Conference 2005

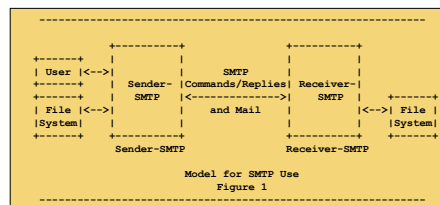


Bug #6: Spam



Retrofitting security is hard to do!

- RFC 821: Simple Mail Transfer Protocol (SMTP)
 - Store-and-forward infrastructure
 - Excellent scalability
- SPAM Problem: **Authentication**
 - No source validation
 - Humans are terrible authenticators
- SPAM Problem: **Economic disparity**
 - Spam costs borne by recipient
 - Similar problem: Telemarketers



Simple Mail Transfer Protocol, RFC 821
Jonathan B. Postel, 1982

RSA Conference 2005



RFC 821

Bug #6: Spam



Retrofitting security is hard to do!

- Other auth. problems

- Cellular AMPS (1983)
- Phishing

(c) SENSE OF CONGRESS.—It is the sense of Congress that—
(1) Spam has become the method of choice for those who distribute pornography, perpetrate fraudulent schemes, and introduce viruses, worms, and Trojan horses into personal and business computer systems; and
(2) the Department of Justice should use all existing law enforcement tools to investigate and prosecute those who send bulk commercial e-mail to facilitate the commission of Federal

S. 877, CAN-SPAM Act

- Anti-SPAM approaches

- Reactive:
 - Filtering, Blacklist, Legislation
- Proactive:
 - Micropayment, proof-of-work
- Infrastructure upgrade: DNS, IPv6

DomainKey-Signature: a=rsa-sha1; q=dns; c=noews; s=beta;
d=gmail.com; h=received:message-id:date:from:reply-
to:to:subject:mime-version:content-type:content-transfer-
encoding;
b=j0v9iv18fxTVjq04gaXJIPSCe0yQehfa61RBoFDCVOMhipXr5bqCh
AlkP4de8BAQ5+pl0V8KfUBQ/RQ8Rcpge5LdXymfCPO9W8MeKmjovX10vi321vK
Qg5aW43xOMBVH8AVYR2MMQm3JUFpivOp0kt8nFXq33WS+q+u82QE7o-
Received: by 13.49.2.55 with SMTP id f55mr13687rni;
Thu, 10 Feb 2005 09:59:08 -0800 (PST)
Message-ID: <74ac93f98654300959312a6ab@mail.gmail.com>
Date: Thu, 10 Feb 2005 09:59:07 -0800

DomainKey email header



RSA Conference 2005

Bug #6: Spam



Retrofitting security is hard to do!

- SMTP: Too well designed to be replaced?

- Infrastructure retrofits are hard!

- Jurisdiction issues: Who's in charge?
- Wide range of proposed solutions
 - Centralized – Authority, dispute resolution, ...
 - Decentralized – Complexity, cheating, ...
- Solutions look to economics
 - Solving the problem of asymmetric costs
 - Incentivize "proper" handling of messages
 - Custom alternate systems



RSA Conference 2005

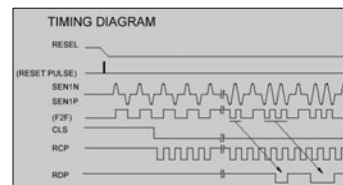
Monty Python's SPAMalot, Eric Idle, 2004

Bug #5: Mag-stripe Skimming



Security technology outlives usefulness.

- Mag-stripes, CC transaction backbone
 - Defined in ISO 7811/2, 7811/4
 - 1960's era technology
 - Cardholder data on read-only tracks 1 & 2
- Fraud begets improvements
 - Revocation: Clerk lookup
 - Online transactions, activation
 - CVC, CVC2: Out of band signaling
- But attacks emerge...
 - Card skimming, cloning



Mag-stripe decoding (F2F)



ATM skimming device

RSA Conference 2005

Source: Uniform Industrial Corp. UCH100 specification



Bug #5: Mag-stripe Skimming



Security technology outlives usefulness.

- Skimming continues to grow
 - In person capture, stripe reading, wiretapping, database theft, ...
- Solutions / Responses
 - New infrastructure required
 - Cryptographic chipcards, tamper resistance, end-to-end security
 - Some proposals silly →

The Fraudulent Device Inhibitor is placed in front of the entrance to the ATM card reader and is designed specifically to prevent an ATM customer from inserting his or her card into the machine if a trapping device has been added to the card reader.

- Good security architectures have 9 (or more) lives
 - Carefully consider incremental improvements
 - Replace the security mechanism if it has outlived its lifespan

RSA Conference 2005

New Cards As Tourists Taken For A Ride, Credit Cards Magazine, February 1, 2005
NCR Demonstrates New ATM Fraud Countermeasure Device, NCR News Release, November 18, 2004

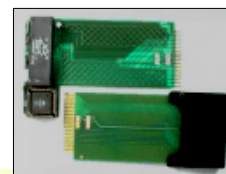
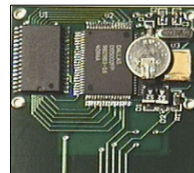
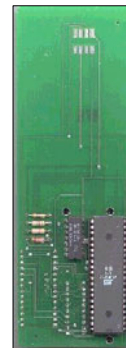


Bug #4: Pay TV Hacking



Repeatable attacks against tamper resistant devices.

- Pay TV
 - Subscription and PPV content
- A profitable target
 - “Test cards” sell for high premiums
 - International boundaries generate demand
- Attackers well equipped
 - Spend significant NRE
 - Reverse engineering, decap, ...
 - Market subsequent attacks
 - Multiple attack vectors
 - SW bugs, protocol failures, debug ports, glitching, ...



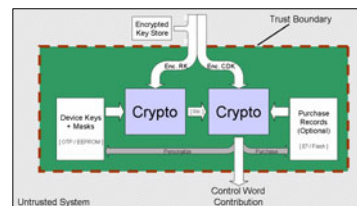
RSA Conference 2005

Bug #4: Pay TV Hacking



Repeatable attacks against tamper resistant devices.

- Apply tamper resistance wisely
 - Goal: make subsequent attacks expensive
 - Manage design complexity
 - Define good security boundaries
 - Design a robust TR core
 - Consistent w/ expected attacks
 - Design should be easy-to-evaluate



Cryptography Research CryptoFirewall™

“Fragile secrets – Handle with care!”
 Building effective tamper resistance
 Friday 11:10am Wireless & Embedded Track

RSA Conference 2005



Bug #3: PC Platform



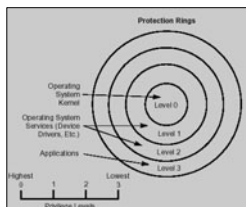
Embrace principle of least privilege.

"f) Least privilege: Every program and every user of the system should operate using the least set of privileges necessary to complete the job."

"The Protection of Information in Computer Systems"
Jerry Saltzer and Mike Schroeder, 1975

Mototola 68000

- Supervisor mode (SRP bit)



Intel 386: Rings 0-3

- Ring 0: Kernel
- Ring 1: System Services
- Ring 2: Custom Extensions
- Ring 3: Applications

Table 3-10. System Control Operation Format

Instruction	Operand Syntax	Operand Size	Operation
ANDI to SR	#data<n>-SR	16	Immediate Data A: SR → SR
EORI to SR	#data<n>-SR	16	Immediate Data @ SR → SR
FRESTORE	<esp>	none	State Frame → Internal Floating-Point Registers

RSA Conference 2005

Intel Architecture Software Developer's Manual Vol 3 (1999)

Motorola M68000 Family Programmer's Reference Manual (1992)



Bug #3: PC Platform



Embrace principle of least privilege.

- What happened?
 - OS support minimal
 - Device driver support abominable
 - Application development functionality-minded
- Lack of compartments begets trouble
 - Worms / viruses / malware not a surprise...but devastation is!
 - Unintended interactions cause a huge fraction of security problems
- "Rolling your own" nearly impossible
 - Shield from hostile code: BIOS, controller chips, INT3s
 - Secure state: Registry tricks, storage volume magic
 - Partitioning: VMware, separate PC + firewall, Citrix

Level 0: Kernel
Level 1: System Services
Level 2: Custom Extensions
Level 3: Applications

80386 Programmer's Reference Manual
Intel Corporation, 1986

RSA Conference 2005



Bug #3: PC Platform



Embrace principle of least privilege.

- Don't sidestep security partitioning
 - Lobby for robust sandboxing
 - Use mechanisms that limit unnecessary interactions
 - Resist urge to bypass protections during development
- It will get better for PC's...
 - New infrastructure: Trusted computing, partitioning, virtualization, ...
- It will get worse elsewhere...
 - "Flat" computing + connectivity + multi-application = DANGER
 - Cellphones, PDAs, entertainment systems...

RSA Conference 2005

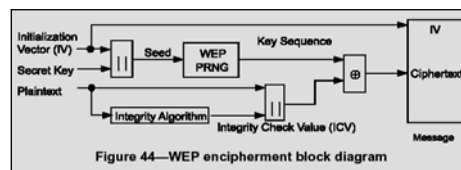


Bug #2: 802.11b WEP



Poor infrastructure causes duplication of security efforts.

- 802.11b WEP: "Wired Equivalent Protocol"
 - Used to encrypt and authenticate packets sent via 802.11b
 - No external review
- WEP protocol horribly broken
 - Integrity check easily bypassed
 - RC4 reseeding on every packet
 - Computationally costly
 - Exposed RC4 weakness
 - Critical pieces missing
 - No key management



RSA Conference 2005



ANSI/IEEE Std 802.11 (1999), MAC & PHY Specifications, p63-64

Bug #2: 802.11b WEP



Poor infrastructure causes duplication of security efforts.

- Corporate IT acceptance of 802.11b held back ~18 months
- Beyond wardriving...
 - Real exploits: Unauthorized network access, database thefts
- Forces duplication of security efforts
 - IT administration, VPN, application level security
 - Challenge: embedded devices that lack UI, other resources
 - NRE of ~\$100M for CRI clients alone

- Create a lasting legacy!
 - Make it hard for users to make security mistakes
 - Get designs reviewed

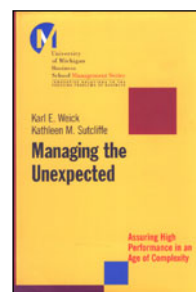
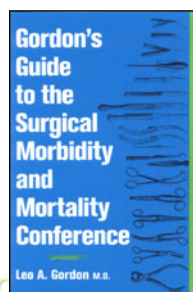
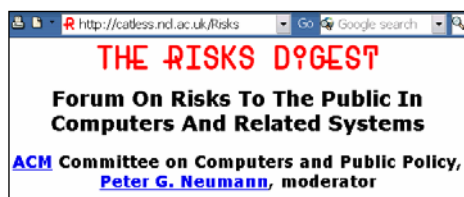
RSA Conference 2005



Bug #1: To the Unknown Bug



How can we fail less than our fair share of times?



RSA C



Questions?



Contact Information

Benjamin Jun
ben@cryptography.com
415.397.0123
www.cryptography.com

We're hiring!

If you are technically strong and want to work on challenging
crypto and security problems, please send a resume!

