INSECURITY ENGINEERING:
ALL SECURITY IS ABOUT LIABILITY

Mechanical engineering

Security engineering

Defective and Deficient designs

Liability

ASSA ABLOY INITIATIVE: "SECURITY THROUGH DESIGN"

- Ensure security and safety of products
- Security engineering in product design phase
- Defined escalation procedures
- Inter-division communications regarding security design issues
- Vulnerability testing in all phases

ISSUES: PRODUCT SECURITY, LIABILITY AND POTENTIAL DAMAGES

- Product deficiency or defects
- Security vulnerabilities
- Deceptive or false claims in customer communications
  - Advertising
  - Manuals
  - Tech support
  - Marketing

SPECIAL RESPONSIBILITY

- YOU ARE NOT MAKING TOASTERS!
- LOCKS ARE A UNIQUE PRODUCT
  - Protect lives, information, property
- CUSTOMERS RELY ON YOUR EXPERTISE IN SECURITY AND DESIGN OF HARDWARE
- SPECIAL COMPETENCE REQUIRED
- UNIQUE ETHICAL STANDARDS
- DISCLOSURE ISSUES

"INSECURITY ENGINEERING": A DEFINITION

- Intersection of mechanical and security engineering
- Must have both mechanics and security
- Must understand bypass techniques and design against at all stages in process
- Develop a new way of thinking
- **Problem: Engineers know how to make things work but not how to break them**

WHAT YOU DO AND HOW YOU DO IT IS CRITICAL

- INSECURE DESIGNS HAVE CONSEQUENCES
  - Potential money damages to company
  - Loss of certification under standards
  - Public relations issues and company image
  - Risk to people and property
  - Advantage to competitors
  - Loss of market share
  - Failure to meet contract and government specifications and standards

MYTHS ABOUT SECURITY AND PRODUCT DESIGN

- It is patented
- Engineers think the produce is secure
- Product has been sold for many years
- No known bypass tools or techniques
- Product meets or exceeds standards
- Testing labs have certified the product
- Government labs say its secure

EXAMPLES OF INSECURITY

- MEDECO: 40 YEARS SECURE
- ASSA and EVVA: WIRE ATTACKS
- KABA SIMPLEX: 35 YEARS SECURE
- SAFLOK WINFIELD: 25 YEARS SECURE
- KRYPTONITE BIKE LOCKS: 15 YEARS SECURE
- PIN TUMBLER LOCKS: BUMPING
- HP COMPUTER LOCKS and EL SAFE
- OTHER HIGH SECURITY LOCKS: 25 YEARS OF INVULNERABILITY

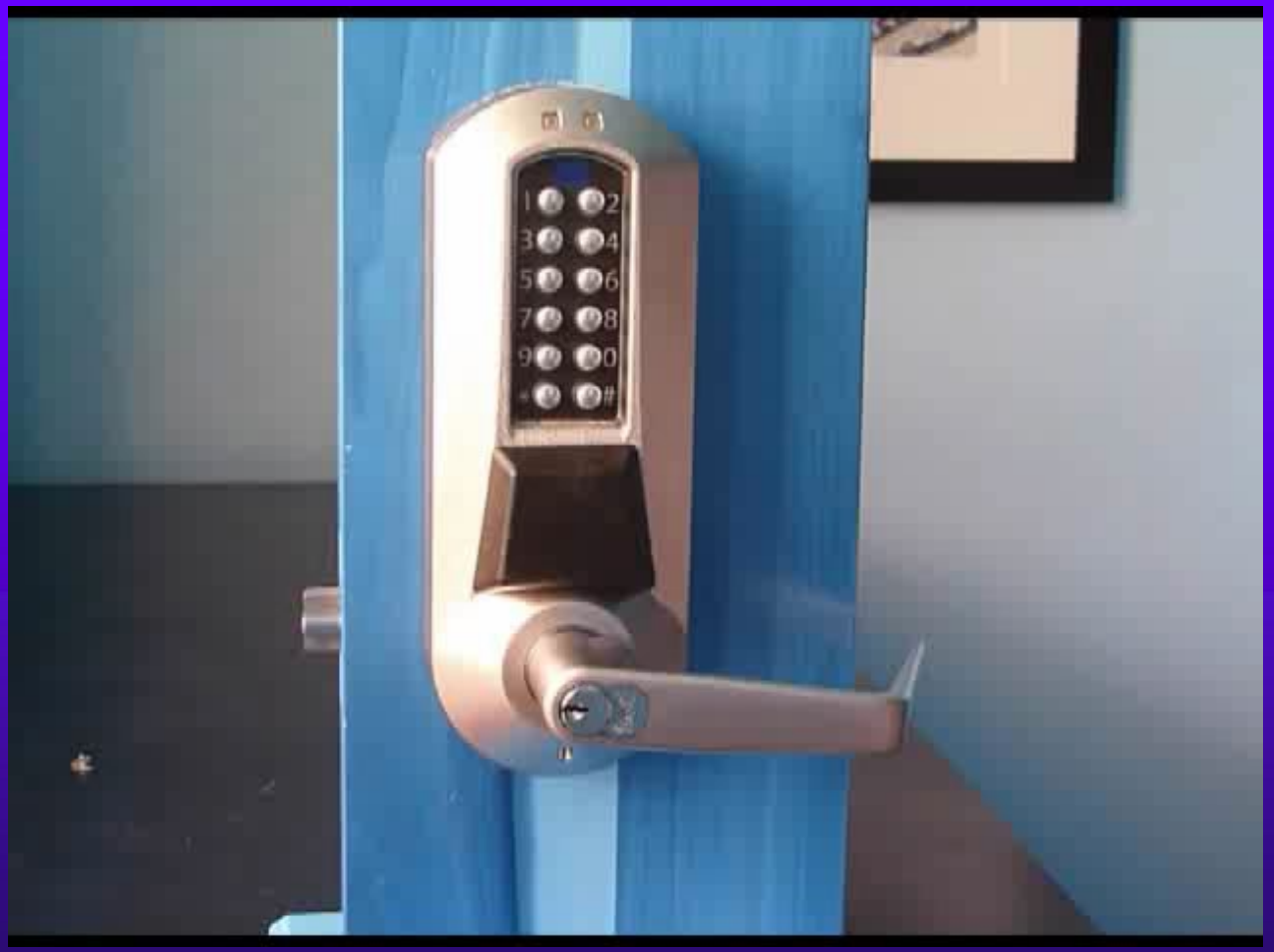
MEDECO CODE SET KEYS: Forty Years of security

KABA SIMPLEX 1000

KABA SIMPLEX DEFECT

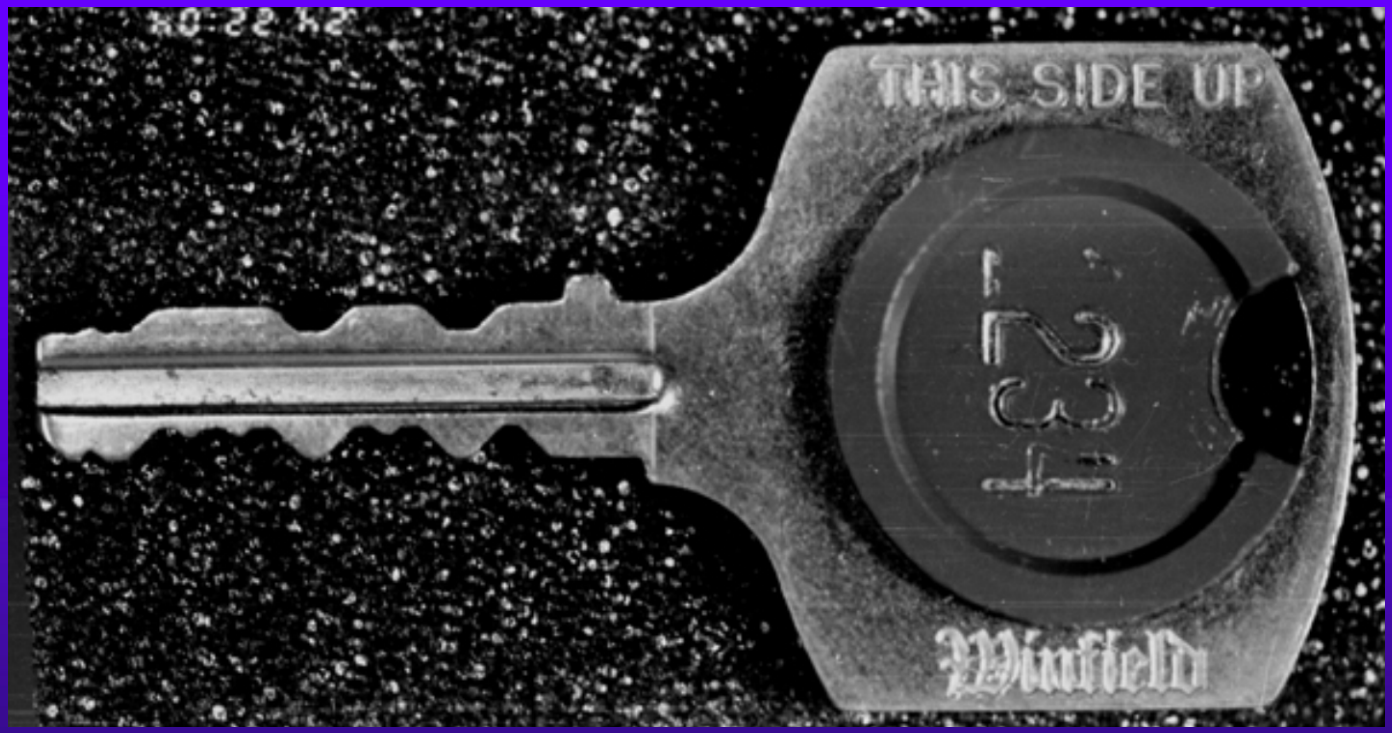
KABA E-PLEX 5000/5800

KABA E-PLEX 5800

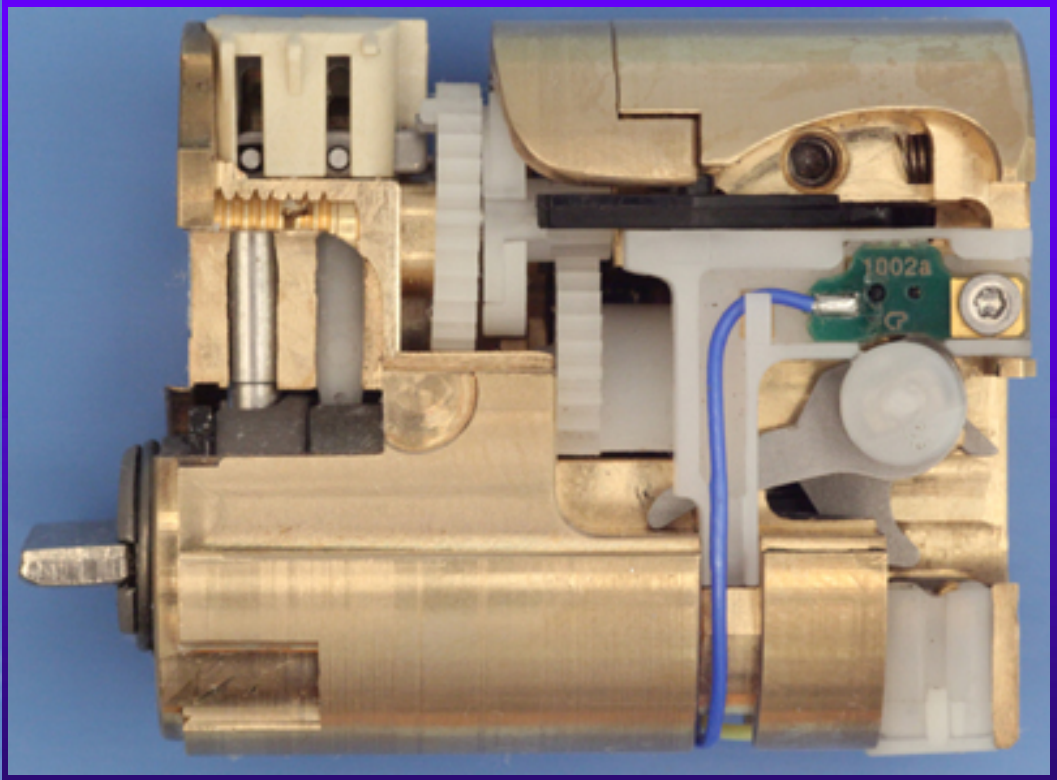


KABA EPLEX 5800 WITH HGH SECURITY CORE

SAFLOK: WINFIELD 20 YEARS OF SECURITY



ILOQ FINLAND: Patented, Award Winning, Insecure



DESIGNS, SECURITY, LIABILITY

- **DESIGN CONTINUUM: Liability v. No Liability**
- State of the Art attack v. Stupid design and simple attack
- REASONABLE INDUSTRY PRACTICE AND KNOWLEDGE INFERRED
- POTENTIAL OR REAL LIABILITY
- COST OF LAWSUITS: MONEY, PR. CREDIBILITY
- COST OF RECALL
- DIFFERENCE BETWEEN LOCKS AND SOFTWARE

LIABILITY v. NO LIABILITY: EXAMPLES

- LOCK BUMPING
- CLIQ WIRE ATTACK
- MAGNETIC ATTACK: KABA SIMPLEX
- MEDECO CODE SETTING KEYS
- KRYPTONITE AND KENSINGTON
- WINFIELD: 1,000,000 HOTEL ROOMS
- VINGCARD MECHANICAL and TESA

"WE MEET THE STANDARDS": SO WHAT!

- LOCK CAN BE OPENED OR NEUTRALIZED IN THIRTY SECONDS
- A 12 YEAR OLD CAN OPEN THE LOCK
- LOCK FAILS OF ESSENTIAL PURPOSE
  - No audit trail
  - No key security
  - Forced entry in seconds

- HYBRID ATTACKS
- Public relations nightmare
- Possible lawsuits

PR AND CORPORATE IMAGE

CLIQ AND SECURITY IMAGE

MEDECO DEADBOLT

POLITICS : SECURITY

Medeco Readies Assembly-Line Fix for DefCon Lock Hack

By Kim Zetter 08.09.07

Researchers were able to bypass the lock inside a Medeco M3 high-security deadbolt to open the deadbolt lock. They say the attack works on any deadbolt, not just those made by Medeco.
Photo: Dave Bullock

High-security lock manufacturer Medeco says it's planning a design change to counter one of two attacks against its products that were described at the DefCon hacking conference over the weekend, boosting security on a line of locks found at the White House, the Pentagon, embassies and other critical locations.

On Sunday, three researchers led by lock-picking expert Marc Weber Tobias showed how they could easily "bump" and pick Biaxial and high-security M3 locks made by Medeco

KABA SIMPLEX 1000

Forbes

Marc Tobias, Contributor

I am an investigative attorney and physical security specialist.

+ Follow

TECH | 2/01/2011 @ 1:52PM | 28,468 views

The $300 Lock You Can Break in Seconds

+ Comment now

The lock you see in the picture at right can be found in thousands of locations: hotels, banks, casinos, office buildings, airports. And, according to a class action lawsuit, it isn't safe at all. Kaba-Ilco, the maker of the ubiquitous Simplex series of push-button locks, is being sued for selling a defective product that can be broken into in seconds by an unskilled person wielding only a powerful magnet. Virtually all of these locks, with the exception of Kaba's Series 5000 model, are vulnerable, according to the complaint filed by the plaintiffs in this case. Kaba is one of the largest lock

tung/2011/08/02/10-questions-do-you-lead-like-rupert-murdoch/

CX5 MEDECO KNOCK-OFF

Forbes

Marc Tobias, Contributor

I am an investigative attorney and physical security specialist.

+ Follow

TECH | 8/22/2011 @ 6:25PM | 920 views

A Medeco Knockoff Lock You Can Open With a $3 Screwdriver

+ Comment now

Earlier this month at Defcon 19 in Las Vegas, we presented an analysis of the Kaba E-Plex series of electronic access control devices as reported by Forbes' Andy Greenberg.

Examining what we perceived as failures in

STANDARDS: THE PROBLEM

- MEET ALL STANDARDS BUT THE LOCK CAN BE EASILY OPENED
  - Not up to date
  - Not incorporate many methods of attack
  - Consumer relies on standards
  - Just because you meet standards does not mean the lock is secure
- MAY WIN ON LIABILITY AND LOSE PR WAR

CORPORATE COMMUNICATIONS AND LIABILITY

- **YOU DON'T KNOW WHAT YOU DON'T KNOW!**
- Must test products against current methods
- Must not overstate: "Ultimate in Security"
- Explain limitations to customers: i.e. MK systems, access control, key security
- Constantly monitor advertising
- Tech support training and monitoring
  - Examples: Medeco and Kaba

INSECURITY IN DESIGNS: ISSUES TO CONSIDER

- Responsible disclosure v. irresponsible non-disclosure and Ethics: Tell the Truth
- Public Relations and press statements
- Obligations to customers
  - Consumer and critical customers
- Liability: disclose v. not disclose of known issue
- Security vulnerabilities: action at what point
- How long are you liable

KABA CASE EXAMPLE: SIMPLEX 1000 AND 5000

- PRODUCT HISTORY
- DISCOVERY OF PROBLEM
- CLASS ACTION LAWSUIT
- RAMIFICATIONS OF LAWSUIT FOR ENTIRE INDUSTRY
- MANY UNSETTLED AREAS OF THE LAW
- IF JURY CAN OPEN THE LOCK
- IF KABA SETTLES

KABA: "ALL LOCKS CAN BE BYPASSED, SO NO LIABILITY"

- SECURITY CONTINUUM
- 3T2R RULE
- IF A 12 YEAR OLD CAN OPEN: IT IS A PROBLEM. ASK MEDECO, or KABA, or KRYPTONITE, or ASSA, or WINKHAUS, or EL SAFE, or VINGCARD……

KABA SIMPLEX PLEADINGS

FILED
IN CLERK'S OFFICE
U.S. DISTRICT COURT E.D.N.Y.
★ NOV 29 2010
BROOKLYN OFFICE

PRESS COPY

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

Aaron Glucksman, Gary Gross, Sylvia Romy, Peter Donato, Individually, and on behalf of all others similarly situated, Plaintiffs, vs. KABA ILCO CORP., KABA CORPORATION, KABA FINANCE CORPORATION, KABA BENZING AMERICA, KABA U.S. HOLDING LTD., KABA DELAWARE, LLC, KABA AG, and KABA HOLDING AG Defendants.	Case No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

GOLD, M.J.

INTRODUCTION

1. This is a nationwide class action on behalf of individuals and business owners who seek compensatory damages, restitution and disgorgement of all profits gained by Defendants arising out of the sale of push button door locks that were designed, manufactured, marketed and sold by Defendants, which contained defects in design that made them susceptible to opening by use of various commercially available magnets, rendering the locks ineffective and unfit to perform the safety function for which they were designed. Each of the aforementioned locks manifests the design defect at the present time. As a result of the defects in design, the locks must be replaced.

2. Plaintiffs also seek remedies for Defendants' failure to adequately notify customers of the defects. Finally, Plaintiffs seek to enjoin Defendants from continuing to engage in the marketing and sale of the defective locks.

LEGAL ISSUES RAISED

- a. Whether the Locks were defectively designed; and
- b. Whether the Locks are not fit for their intended use; and
- c. Whether the Defendants failed to wam of the ability for the safety mechanism of the Locks to be bypassed; and
- d. Whether the Defendants concealed information and the nature of the defects from the Class Members; and

LEGAL ISSUES RAISED

- e. Whether Defendants engaged in the alleged conduct knowingly, recklessly, or negligently; and
- f. The amount of revenues and profits Defendants received andlor the amount of monies or other obligations lost by Class Members as a result of such wrongdoing;
- g. Whether Class Members are entitled to declaratory, injooctive and other equitable relief and, if so, what is the nature of such relief; and
- h. Whether Class Members are entitled to payment of actual, incidental, consequential, exemplary andlor statutory damages plus interest thereon, and ifso, what is the nature of such relief;

CAUSES OF ACTION

- NEGLIGENCE
- STRICT PRODUCT LIABILITY
- FAILURE TO WARN
- BREACH OF WARRANTY
- CONSUMER PROTECTION STATUTES
- Unfair competition or deceptive trade
- COMMON LAW FRAUD
- UNUST ENRICHMENT
- DECEIPT, FRAUD, MISREPRESENTATION
- NEGLIGENT MISREPRESENTATION
- VIOLATION OF FEDERAL WARRANTY ACTS
- REPLACEMENT AND NOTIFICATION PROGRAM

WHAT YOU NEED TO DO

- THINK OUT OF THE BOX
- FIRST RULE: “THE KEY NEVER UNLOCKS THE LOCK”!
- MECHANICAL AND SECURITY ENGINEERING TOGETHER
- COMPONENT FAILURE ANALYSIS
- WHAT WE DO IN OUR LAB
- CONSTANTLY MONITORAND TEST
- UNDERSTAND BYPASS TECHNIQUES

EMEA STOCKHOLM 2011 LIABILITY AND SECURITY

- mwtobias@security.org
- 1.605.334.1155