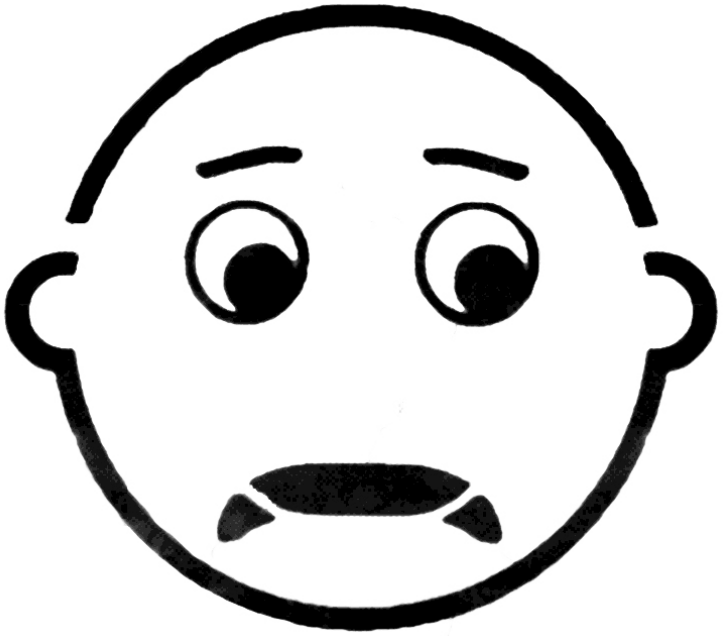
Invisible Access



Opening New Doors to Insecurity

Marc Weber Tobias - Matt Fiddler - Tobias Bluzmanis

©2009 Security.org

Agenda

- Standards and Requirements
- Electro-Mechanical Locks
- Critical Infrastructure and Vulnerabilities
- Real World Threats
- Case Study: Electronic Access Control technology

in.Security.Org
Knowledge is Security

Standards: Mechanical Locks

- Why we need Standards
- What They Measure
- Limited Protocol - Few Tests
- Exclude many “Real World Attacks”
  - Bumping
  - Mechanical Bypass
  - Knowledgeable and Special Attack Techniques - Not Contemplated

in.Security.Org
Knowledge is Security

Security Criteria: Standards

- Define Conventional vs. High Security
- Threat Criteria
  - Forced Entry
  - Covert Entry
  - Key Security
- All Standards based upon
  - Time, Tools and Training

inSecurity.Org
Knowledge is Security

Forced Entry
UL437 and BHMA 156.30

- Locks must be secure against Forced methods of Attack
- Attack Resistance 5 Minutes
- Excludes many methods of attack

in.Security.Org
Knowledge is Security

Covert Entry Protection

- Minimum Security Criteria in UL437 and ANSI/BHMA 156.30
- Protects against Certain forms of Covert Entry
- Assures Minimum resistance to opening
  - (10 - 15 minutes)
  - Picking and Decoding
  - Master Key Attacks
  - Bumping (Not Covered)

inSecurity.Org
Knowledge is Security

Key Security

- Organizational Protection
  - Duplication of Keys
  - Keys Ordered by Code
- Legal Protection
  - Availability of Blanks
- Does not address Technical Security of Keys
- Standards = Limited Security

in.Security.Org
Knowledge is Security

Categories of Locks

- Conventional Mechanical Locks
- High Security Mechanical Locks
- Electronic Credentials
  - Electro-Mechanical Locks
  - Electronic Locks
  - Wired, Wireless, Data on Card

in.Security.Org
Knowledge is Security

Critical Questions

- What is SECURITY re: Locks?
- Is it secure enough?
- What does a High Security rating mean?
- The concept of key control, key security and why it's important
- Can the lock be compromised and how difficult is it?
- Real World Threats
- Methods to Compromise

in.Security.Org
Knowledge is Security

Conventional Lock Functions

- Restrict “WHO” can enter
- Prevent or Delay Unauthorized Access
  - Low to Medium security
  - Not Certified
  - Covert Entry often is easy

in.Security.Org
Knowledge is Security

Conventional Lock Vulnerabilities

- Picking, Bumping, Decoding
- Impressioning
- Master Key Extrapolation
- Mechanical Bypass
- Failure of Key Control
  - Duplication of keys
  - Simulation of Keys
  - Replication of Keys

in.Security.Org
Knowledge is Security

Conventional Locks:
Adequate for critical applications?

- No tracking of access, attempts, how often or when
- Add or Duplicate keys
- Key Security
- Master Key System Insecurity
- No evidence of Breach
- No Intelligence in lock or key

in.Security.Org
Knowledge is Security

Conventional v. High Security Mechanical

- Conventional Cylinders
  - Easy to Pick or Bump open
  - No Key Control
  - Limited Forced Entry resistance
- High Security Cylinders
  - UL and BHMA/ANSI Standards
    - UL-437 and BHMA/ANSI 156.30
  - Higher quality and tolerances
  - Resistance to Forced and Covert Entry
  - Key Control

in.Security.Org
Knowledge is Security

High Security Increased Protection?

- Protect high value targets
- Stringent security requirements
- Standards (UL and BHMA/ANSI)
- Threat Level is higher
- Minimum security criteria
  - Attack times and resistance
  - More difficult to compromise
  - Higher key control

in.Security.Org
Knowledge is Security

High Security Critical Differences

- Multiple security layers
- More than one point of failure
- Each security layer is independent
- Security layers operate in parallel
- Difficult to bypass each layer
- Difficult to derive intelligence about a layer
- Difficult to simulate the action of a key

in.Security.Org
Knowledge is Security

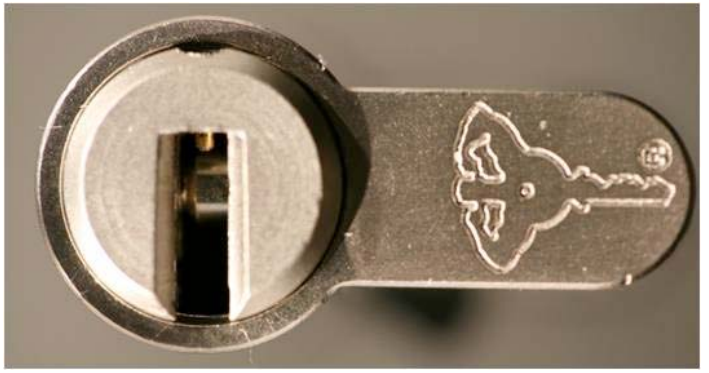
Mechanical Locks: Design Limitations

- Good for one person, one key
- No Key / User Tracking
- Addition of deletion of keys to the system
- Lost stolen or copied keys
- Manipulation of keys (Mul-T-Lock and key interchange issues)

in.Security.Org
Knowledge is Security

Electronic Locks: The Security Solution?









Electro-Mechanical Locks

- Mechanical Locks + Electronic Credentials
  - STILL Mechanical Locks
- Two Parallel Locking Systems
  - Mechanically keyed alike
  - Mechanically master-keyed
  - Key bitting assigned to each customer

in.Security.Org
Knowledge is Security

Electronic Access Control Systems

- Mechanical lock designs
- Electronic Credentials
  - I-button, RFID, SmartCard
  - Many different protocols
- Security Layers
  - Protocol
  - Mechanical locking system
  - Audit Functions
  - Key Security

in.Security.Org
Knowledge is Security

CLIQ® TECHNOLOGY
Higher Security?

ASSA ABLOY COMMON DESIGN

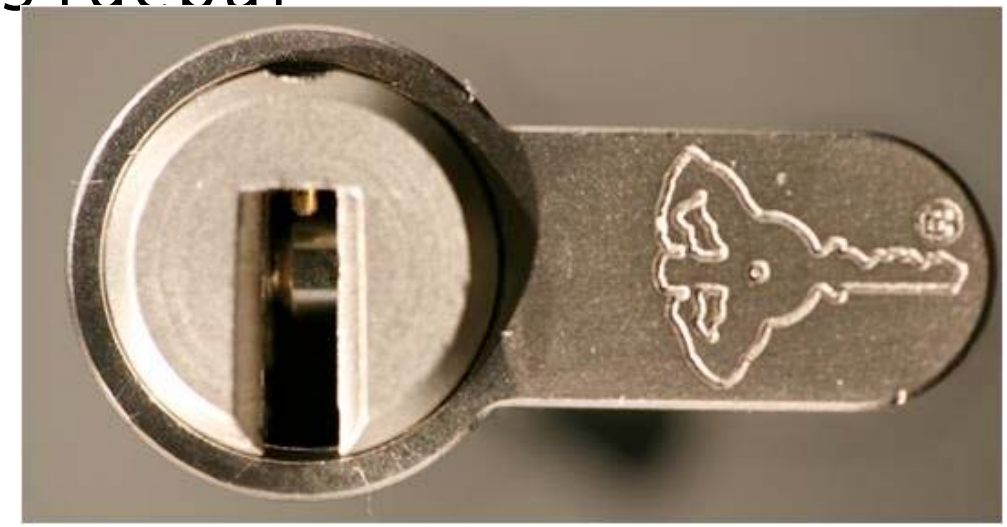
- MEDECO LOGIC
- ASSA CLIQ
- IKON VERSO
- MUL-T-LOCK CLIQ
- OTHERS

in.Security.Org
Knowledge is Security

CLIQ LOCKS:

Mechanical Locks + Electronic Controlled Mechanical Locking Sidebar



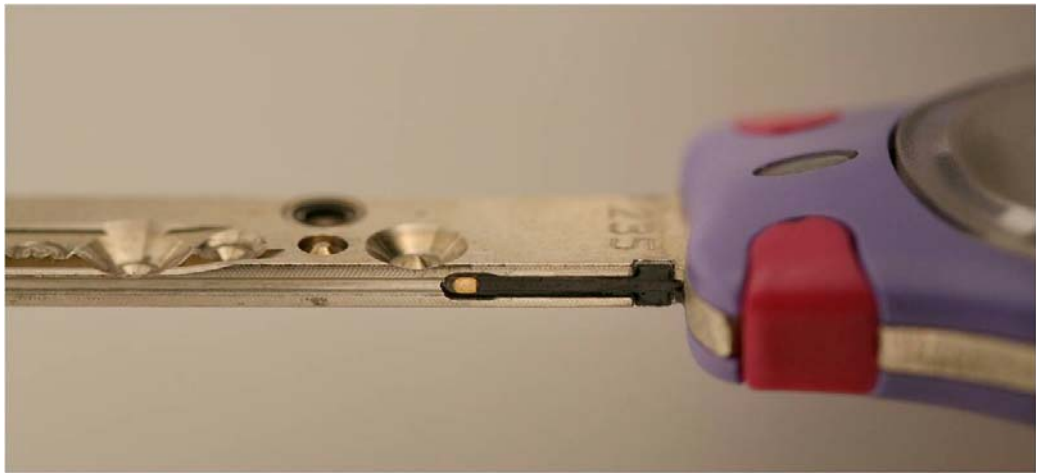




in.Security.Org
Knowledge is Security

CLIQ KEYS:
BITTING + ELECTRONICS





in.Security.Org
Knowledge is Security

ASSA DP SOLO CLIQ



in.Security.Org
Knowledge is Security

Critical Infrastructure

- Transportation - Aviation and Airport Security
- Cargo and Transport
- Power Facilities
- Finance and Banking
- Server Rooms
- Defense
- Public Safety
- Schools

in.Security.Org
Knowledge is Security

CI: Vulnerabilities

- Intrusion (Sabotage and Vandalism)
- Theft of Critical and High Value Targets
- Terrorism
- Data Leakage
- Identity Theft
- Interruption of Critical or Essential Services

in.Security.Org
Knowledge is Security

Airports and Aircraft



in.Security.Org
Knowledge is Security

Aviation Security

- US Aviation Transportation Security Act (2001)
- Defines Requirements for: Airports, Highways, Buses, Ports, Mass Transit
  - Controls Physical Access for 450 Airports
  - Control, Track and Analyze Individual Access and Attempts to Secure Areas

in.Security.Org
Knowledge is Security

Airport Security

- Section 106: Airport Perimeter Protection
- Security Technology to manage Access Control
- Positively Verify the Identity of each Employee and Law Enforcement Officer
- Test and Assure Compliance

inSecurity.Org
Knowledge is Security

Airport Security

- Layered Security Approach
- Physical Security of Fixed Assets
- Beaches: Trace directly to Lock and User Violations
- Copying Keys

in.Security.Org
Knowledge is Security

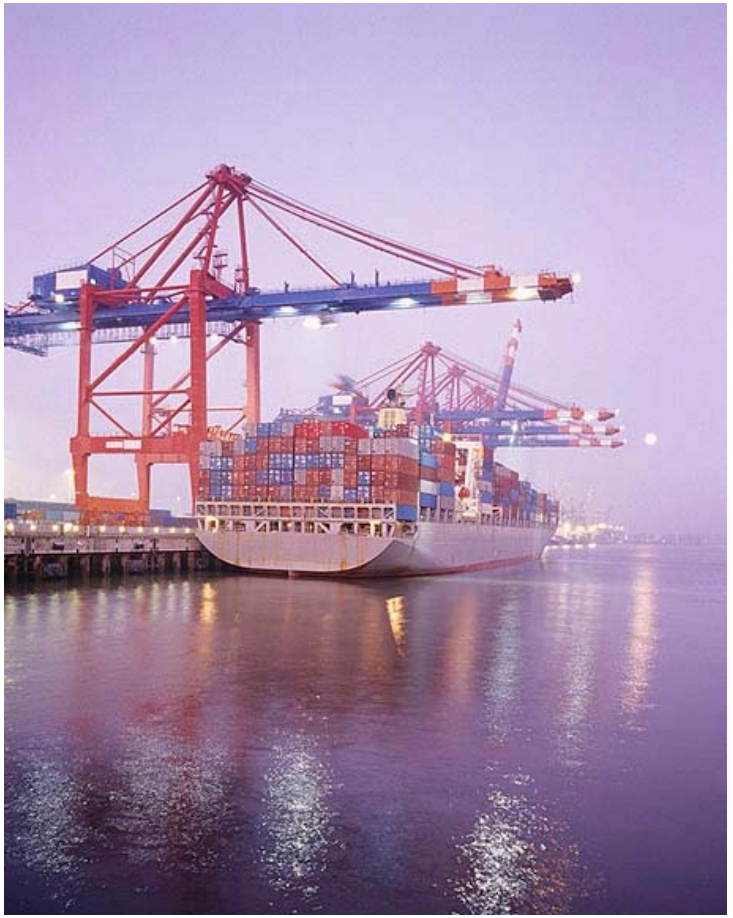
Conventional Locks <u>Not Secure</u> for Airport Protection

- Duplication of Keys
- No User-Auditable Information
- No Scheduling Capabilities (Time Lock)
- Master Key Systems:
  - No Identification of Employee or Ability to Test System

in.Security.Org
Knowledge is Security

Cargo - Containers





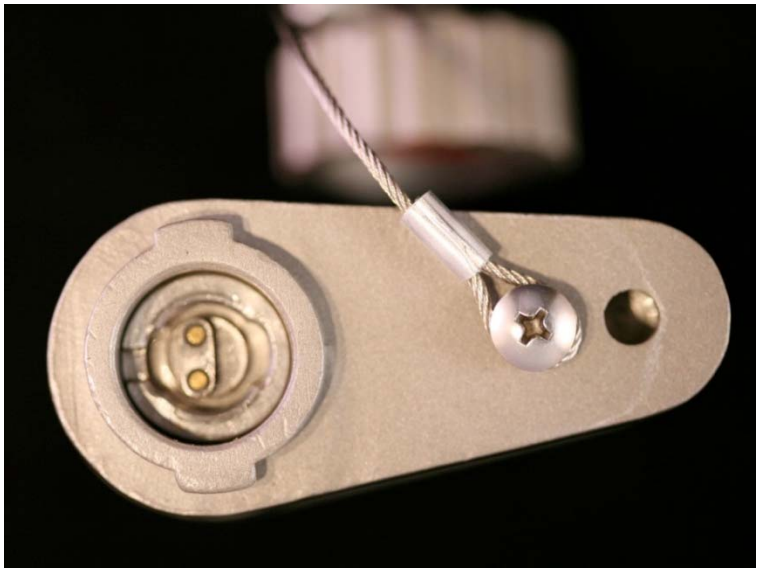
in.Security.Org
Knowledge is Security

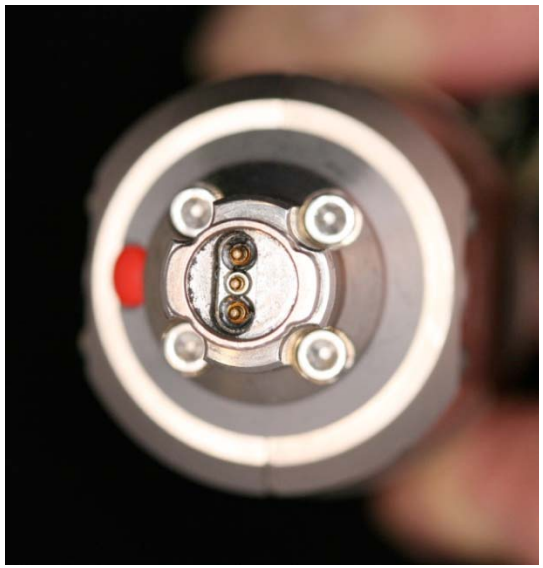
Cargo - Access

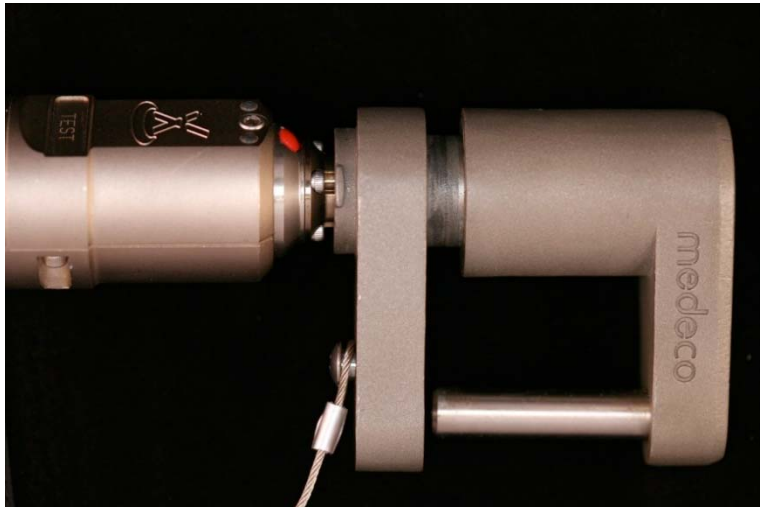
- Electronic Access Control Systems
- Electronic Padlocks with Audit Capabilities
  - Identify Tampering
  - Deter Contraband Introduction and other Attacks

in.Security.Org
Knowledge is Security

Medeco NexGen

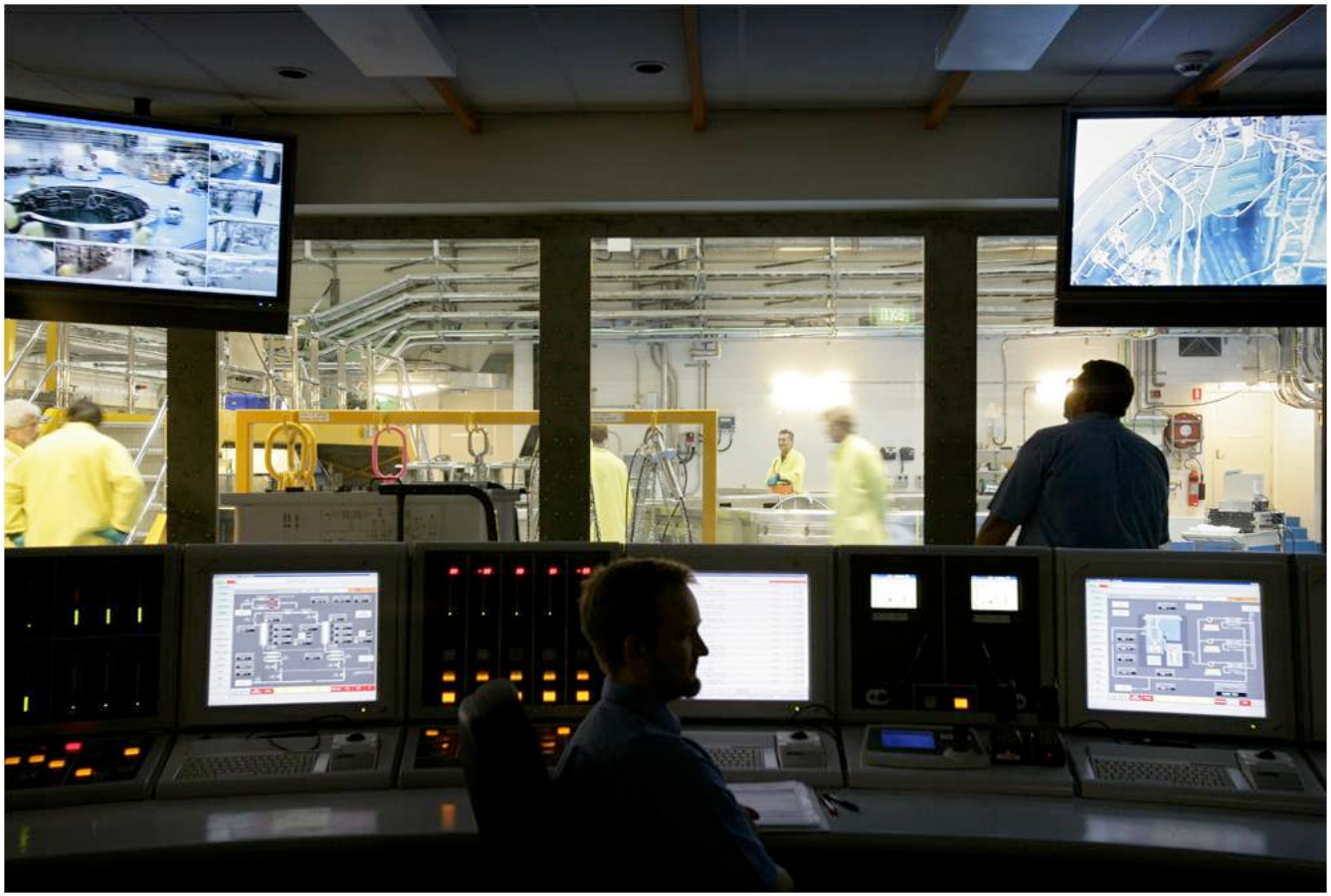






in.Security.Org
Knowledge is Security

Power Generation



in.Security.Org
Knowledge is Security

Power Plants

- Gas, Oil, Power-Grid
- Federal Energy Regulatory Commission (FERC)
- North America Electric Reliability Corporation (NERC)
- Reliability of Electricity
  - Security of Physical Assets
  - Security of Electronic Data

in.Security.Org
Knowledge is Security

Security Requirements

- Prevent Attacks (Both Physical and Electronic)
- Access to Data and Equipment
  - Hard Assets: Generating Plants,Equipment,Transmission, Networks
  - Physical Access and Attempts

in.Security.Org
Knowledge is Security

Critical Infrastructure Protection

- CIP-006-1:

  The Physical Security Plan must:

"Contain procedures for identifying, controlling and monitoring all access points and authorization requests."

"Logging of Physical Access must occur at all times and the information logged must be sufficient to uniquely identify individuals"

inSecurity.Org
Knowledge is Security

Financial Data

- Sarbanes Oxley Act (2002)
  - Financial Reporting for Public Corporations
  - Quality of Financial Reporting
  - IT and Internal Controls
  - Data Center Access Security

inSecurity.Org
Knowledge is Security

Financial Data Integrity and Security

- Control and Safeguard Data
- Validity of Financial Reports
- Physical Control of Access to Information
  - Data Protection
  - Theft
  - Manipulation or Exploitation
  - Unauthorized Access

in.Security.Org
Knowledge is Security

Data Center Security

- Must Control Physical Access to servers to Protect Data
- Electronic Access
  - Passwords, Firewalls, IPS, Encryption

  Physical Access = Game Over

in.Security.Org
Knowledge is Security

Real World Threats

- High Security Locks
- Electronic Access Control Systems
  - Total Compromise
  - False Sense of Security
  - Liability?

in.Security.Org
Knowledge is Security

2007-2008: Our Research

- High Security Lock Vulnerabilities
- Total Compromise of Covert and Forced Entry within Medeco locks, including a total failure of Key Control

in.Security.Org
Knowledge is Security

2007-2008













in.Security.Org
Knowledge is Security

Mechanical Locks

Too Many Limitations

- Good for One Person - One Key
- Used where no tracking is required
- Addition or Deletion of Keys not a requirement
- No concern over Lost or Stolen Keys

in.Security.Org
Knowledge is Security



Electronic Access Control

- The Answer to Mechanical Locks?
- Current Systems
  - Mechanical + Electric
  - All Electronic
    - Wired
    - Data on Card
    - Wireless

in.Security.Org
Knowledge is Security

Stand-Alone EAC

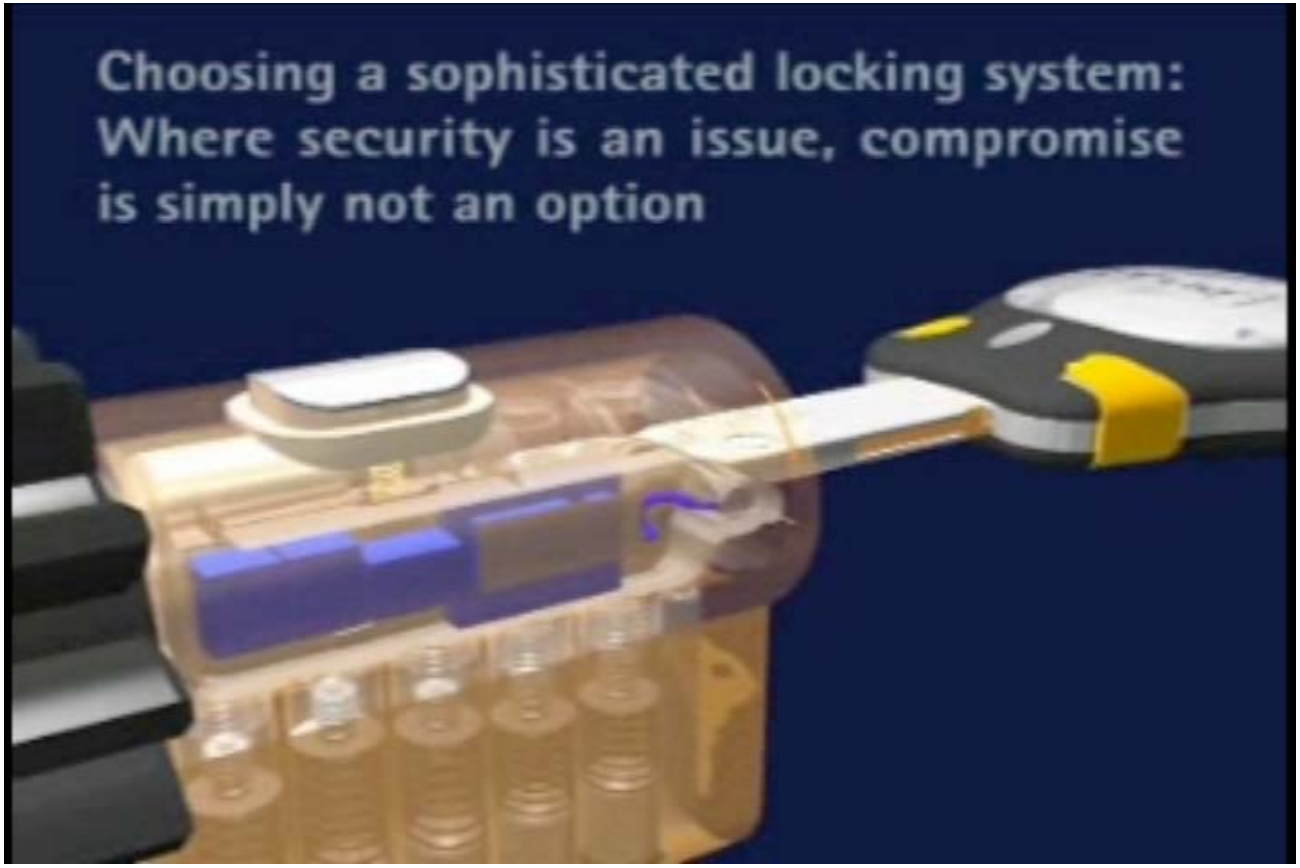
(Assa Abloy Cliq)

- Mul-T-Lock, Assa, Ikon, Medeco Logic
  - All SAME Core Technology!
- Electromechanical Stand-Alone Cylinder
- Mechanical Locking + Audit
- Enhanced Control Options
- Used Throughout the World

in.Security.Org
Knowledge is Security

Mul-T-Lock

“The Ultimate in High Security”



in.Security.Org
Knowledge is Security

LOGIC and Cliq: Design Attributes

- Program Permissions
- Authorized Keys
- Audit Trail Events
- Mechanical + Electronic Security
- No Wiring or additional hardware required

in.Security.Org
Knowledge is Security

Cliq and Logic

- Key Powers the Lock
- Mechanical Bitting + Credentials
- Easy Retrofit to Existing Locks
- Add and/or Delete keys
- Wide range of Access Controls
  - Time, Date, Door (Lock), User, etc.

in.Security.Org
Knowledge is Security

Assa Abloy and EAC: Security and Reality

- Key Control
  - Simulation of Keys
  - Lost, Stolen, or Deleted Keys
  - Entire System at Risk
  - Cannot Re-Key some Cylinders
- Simulate Credentials
- Bypass ALL Audit Functions

in.Security.Org
Knowledge is Security

SERIOUS SECURITY ISSUES: Audit Trail

- False Sense of Security
- Ability to bypass
- Potential for False Blame
- No Evidence of Entry
- Total Lack of “Chain of Custody”

in.Security.Org
Knowledge is Security

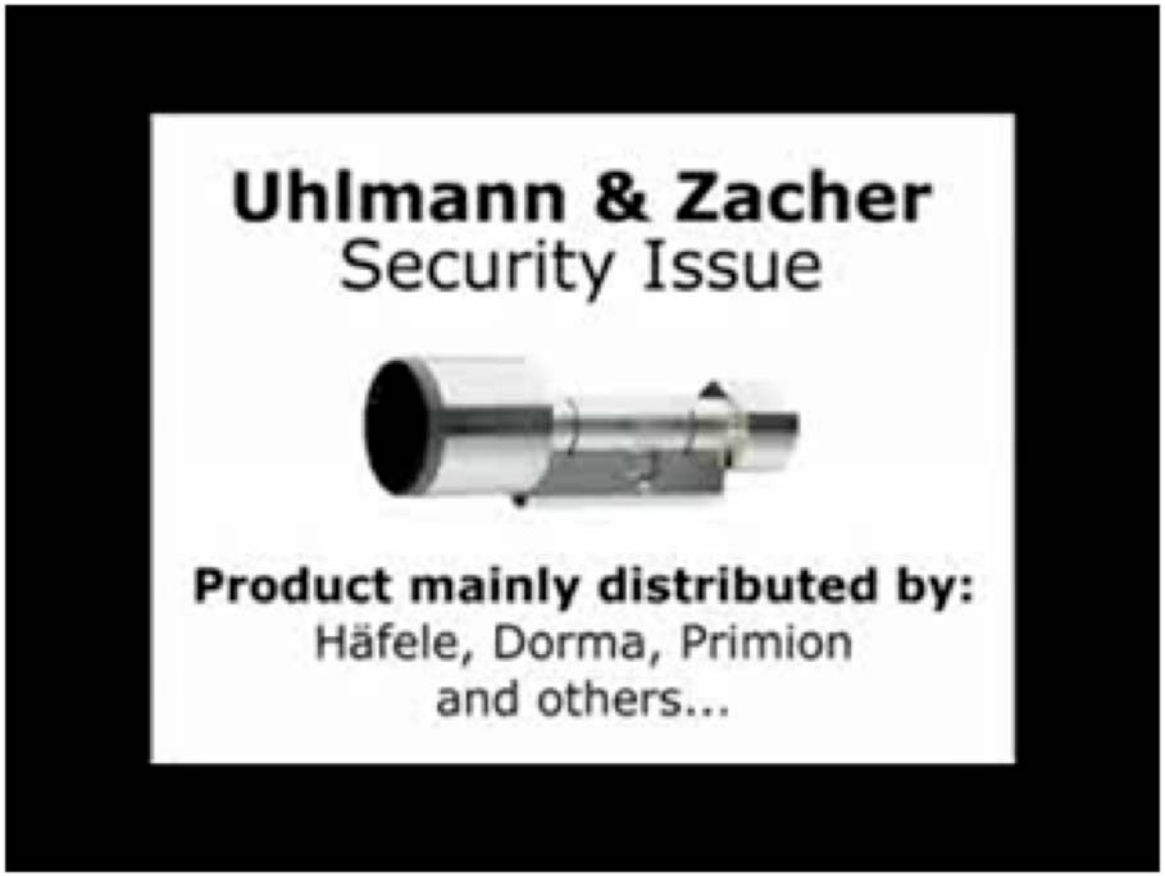
EAC Vulnerabilities

- Bypass of Mechanical or Electronic System
- Audit trail Depends on Reading the Key

What Happens if one Layer is Bypassed?

in.Security.Org
Knowledge is Security

Magnetic Attacks
Ulmann Zacher



in.Security.Org
Knowledge is Security

Cliq and Logic Security Issues: Keys

- Mechanical Keys
- Wafer or Pin Tumbler Systems
- Often "Keyed Alike" Systems
  - Keys Only cut at Factory
  - Electronic Technology inside Key
- Mul-T-Lock results of Keyed Alike and Key Duplication

in.Security.Org
Knowledge is Security

Cliq and Logic Simulated Credentials

- Possess Key and Simulate or Bypass Credentials

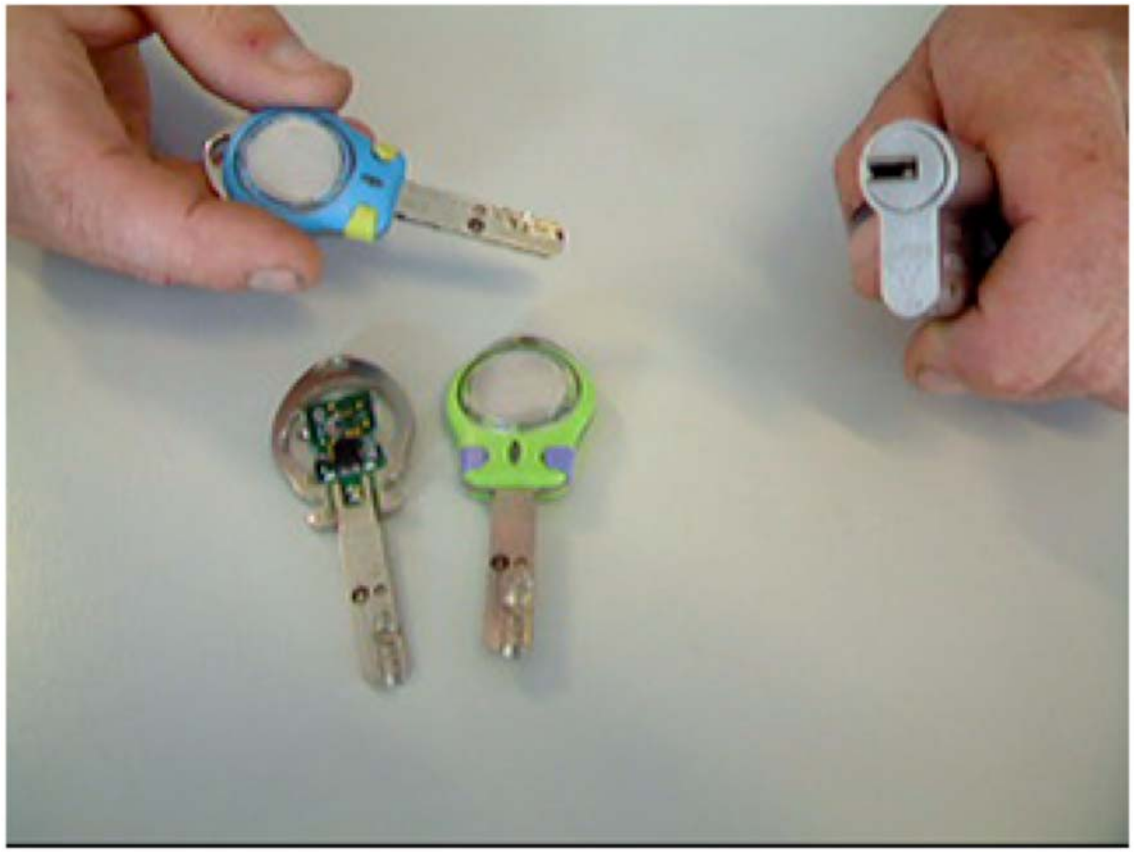
One Lost Key in Key Alike system

=

Total Compromise of System!

in.Security.Org
Knowledge is Security

Mul-T-Lock Click and Magnets



in.Security.Org
Knowledge is Security



Invisible Access Audit Trail Bypass

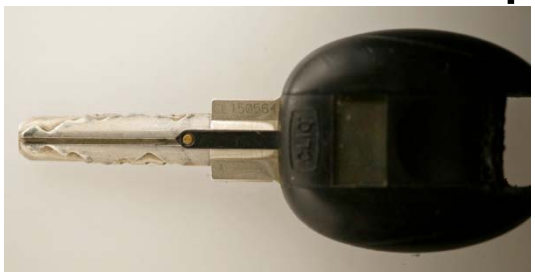
- Audit trail is dependent upon reading the Lock or Key
- If there is NO Audit Trail:
  - False Sense of Security
  - False Blame
  - Unknown Compromise
  - No Evidence of Entry

in.Security.Org
Knowledge is Security

Cliq and Logic Security

From Medeco:

"Unauthorized Key Copying is removed from the Equation"



"Superior Protection against Unauthorized Key Copying"

in.Security.Org
Knowledge is Security

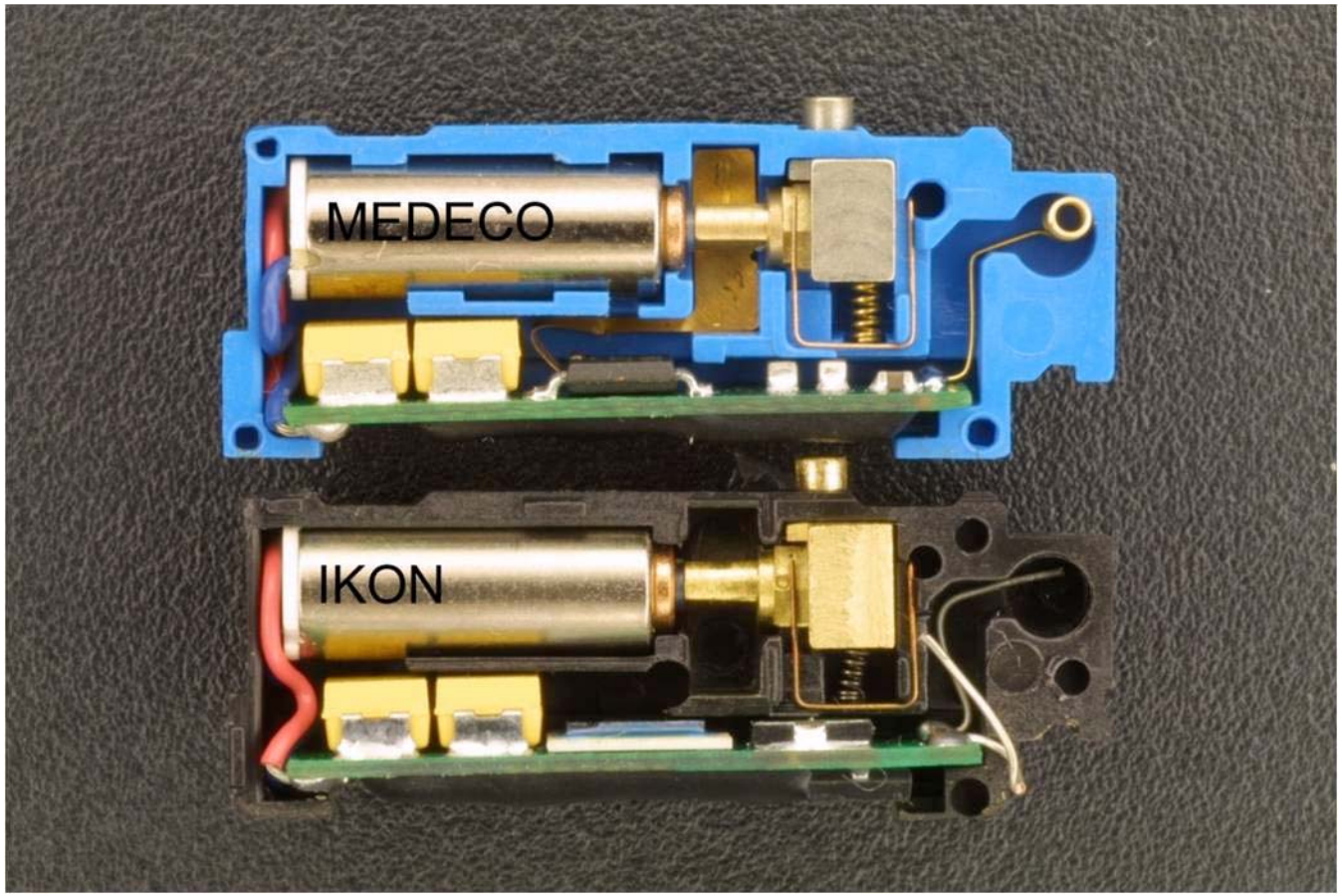
Cliq, Logic and Nexgen Potential Issues

- One lost, stolen or deleted key may compromise entire system
- Simulation of Credentials
- Simulation of Keys
- Open in 30 seconds or less
- No Audit Trail

<u>Invisible Access</u>

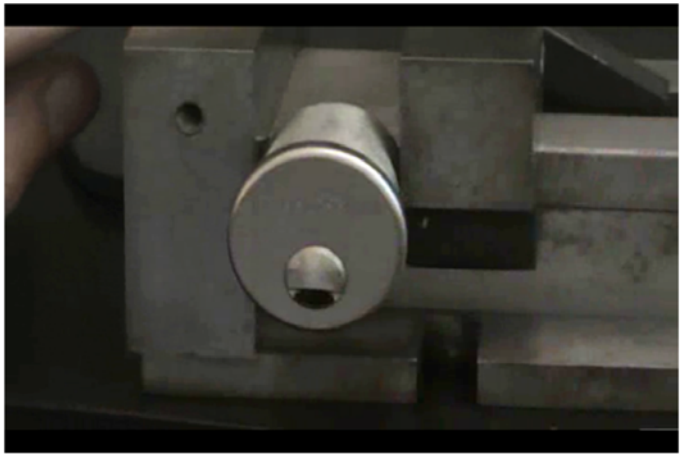
in.Security.Org
Knowledge is Security

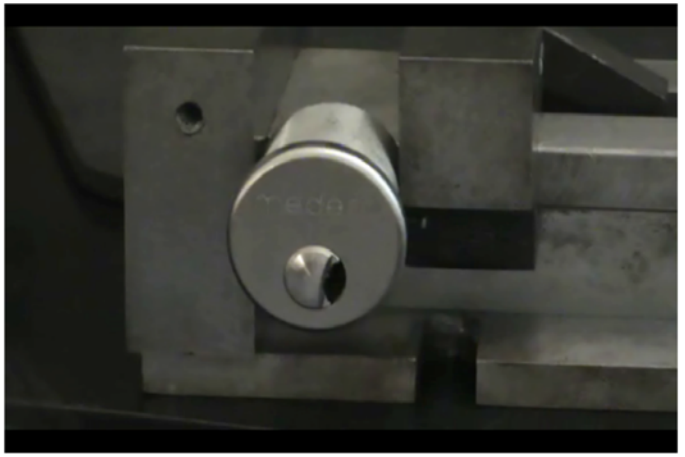
LOGIC Design

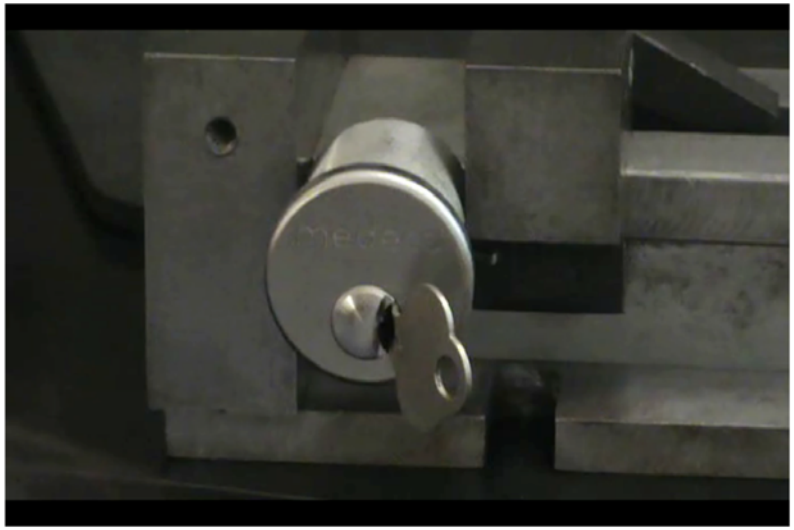


in.Security.Org
Knowledge is Security

Logic In-Security
Simulated Keys







in.Security.Org
Knowledge is Security

Cliq Compromise



in.Security.Org
Knowledge is Security

EAC-Serious Issues

- Mechanical Bypass
- Simulation of Credentials
- Bypass of Electronics
- Cloned Credentials
- Defective Security Design
- Failure to meet Statutory Requirements
- Legal Liability
- Compromise of Entire System

in.Security.Org
Knowledge is Security

SECURITY ENGINEERING ISSUES

- MECHANICAL DESIGN V. SECURITY
  - COMPETENT SECURITY ENGINEERING?
- COMPROMISES IN DESIGN
- HIGH SECURITY INSTALLATIONS
- FACILITY LIABILITY ISSUES
- STATUTORY REQUIREMENTS
- LEGAL LIABILITY TO CUSTOMERS

in.Security.Org
Knowledge is Security



2009 RESEARCH
ELECTRO-MECHANICAL LOCKS

- BEGUN BY TOOL IN EUROPE
- CONTINUED IN THE U.S.
- **WE EXAMINED AND ANALYZED**
  - DESIGN OF CLIQ TECHNOLOGY
    - KEY CONTROL
    - MECHANICAL BYPASS
    - SIMULATION OF ELECTRONICS
  - MANUFACTURER REPRESENTATIONS
  - SECURITY AGAINST INSIDER AND OTHER ATTACKS

in.Security.Org
Knowledge is Security

CONTACT WITH ASSA ABLOY IN 2009

- GENERAL COUNSEL FOR ASSA ABLOY, MEDECO, MUL-T-LOCK
- NOTIFY OF SECURITY DESIGN DEFECTS
- **OUR OFFER: LOCKS, DATA, FIX**

- **THEIR RESPONSE:** NO LOCKS, DEMAND INFO, NOT POLICY TO RETROACTIVELY FIX SECURITY

in.Security.Org
Knowledge is Security

SECURITY ENGINEERING: Defective Designs

- WHAT CONSTITUTES SECURITY DEFECT?
- SECURITY V. MECHANICAL DEFECTS
- STATE OF THE ART v. SIMPLE ATTACK
- WHO SHOULD BE LIABLE?
- ASSA ABLOY POLICY

in.Security.Org
Knowledge is Security

SECURITY ENGINEERING DEFECTS: MEDECO

“But that doesn't tell you what to do if you've got a potentially vulnerable Medeco lock. Don't count on Medeco to replace it: "When you buy a lock, you don't buy a subscription," Roberson told me. Instead, he counseled, people should visit experts and determine their security needs.”

(Slate.com 5/23/2008)

in.Security.Org
Knowledge is Security

STATEMENTS: SECURITY ENGINEERING ISSUES

- MUL-T-LOCK
- “You have misrepresented that Mul-T-Lock's policy is not to consider replacing or repairing a product which proves to be defective in normal use. This is a gross misrepresentation and not true.”
- (7/31/2009)

in.Security.Org
Knowledge is Security

STATEMENTS: SECURITY ENGINEERING ISSUES

ASSA ABLOY:

“All of your accusations and unreasonable demands seem to stem from your mistaken or feigned belief that because a product may under certain limited circumstances be susceptible to a new form of attack. it is somehow rendered "defective.“

(5/15/2009)

inSecurity.Org
Knowledge is Security

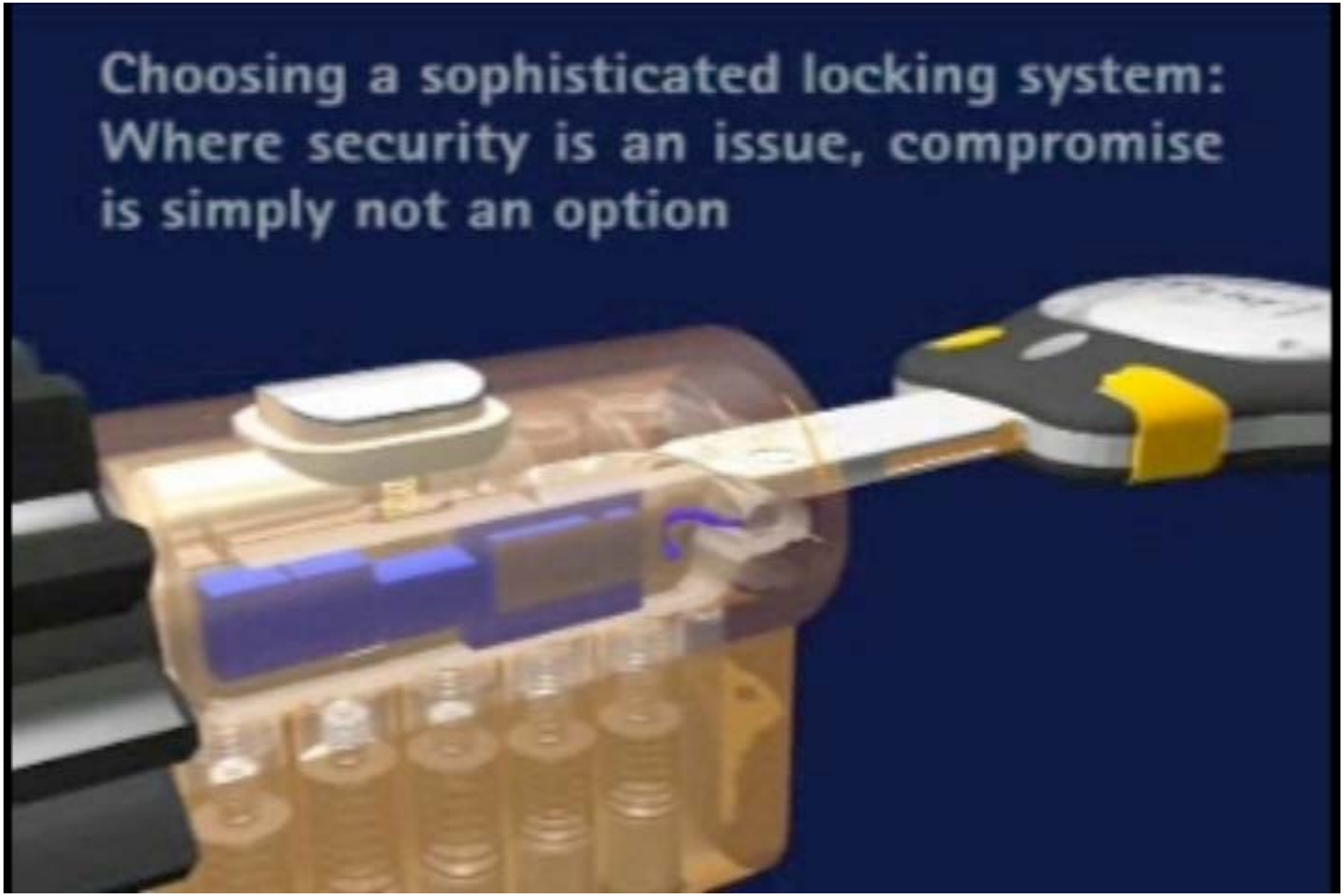
DEFECITVE PRODUCT AND SECURITY ENGINEERING

- QUESTIONS:
- Mechanical defects v. Security defects: is there a difference?
- Should a manufacturer be liable for defective security engineering if it is not a state of the art attack and should have been foreseen?

in.Security.Org
Knowledge is Security



MUL-T-LOCK CLIQ



MUL-T-LOCK CLIQ: ADVERTISING

"In a world increasingly challenged my mounting security threats, the need for comprehensive locking systems has become an essential requirement in virtually every conceivable market sector."

in.Security.Org
Knowledge is Security

STATEMENTS BY MUL-T-LOCK

"Each interactive Cliq key contains a unique electronic ID code. It is designated for one individual only, and cannot be duplicated, altered, or corrupted. "

"If the key is not authorized, the mechanical element in the locking system will simply remain locked."

in.Security.Org
Knowledge is Security

MUL-T-LOCK CLIQ SECURITY

"Intreractive Cliq: unprecedented benefits. The dual patent-protected technologies employed in interactive Cliq represent a truly successful marriage of electrical and mechanical locking systems offering a double layer of **impenetrable security**."

in.Security.Org
Knowledge is Security

MUL-T-LOCK CLIQ: AUDIT TRAIL

"Audit trail control is an absolute necessity if you hope to keep tabs on the **efficacy** of your locking network…. Interactive Cliq's control key enables you to easily access precise data from every cylinder in your facility…each key is designated for use by one individual only. If the key is lost, it is simply made obsolete…This enables total control of every key issued to personnel. "

inSecurity.Org
Knowledge is Security

MUL-T-LOCK CLIQ SECURITY

"Interactive Cliq: launching electro-mechanical locking systems to the ultimate level of security."

in.Security.Org
Knowledge is Security

RESEARCH FINDINGS

- ANALYZED DIFFERENT CLIQ VERSIONS
  - MEDECO LOGIC
  - ASSA TWIN
  - ASSA DP SOLO (Not in U.S. yet)
  - IKON VERSO
  - MUL-T-LOCK

in.Security.Org
Knowledge is Security

EDITED COMPOSITE VIDEO Different Attacks

- VULNERABILITY BUT NOT METHODS
  - LOCKS USED IN CRITICAL APPLICATIONS
- DISCLAIMERS
  - DIFFERENT VERSIONS, MAY NOT ALL REACT THE SAME
  - MAINLY INSIDER ATTACKS
  - OUR OPINION: SERIOUS VULNERABILITIES. DEPENDS ON APPLICATION
  - OUR OPINION: INCOMPETENT ENGINEERING



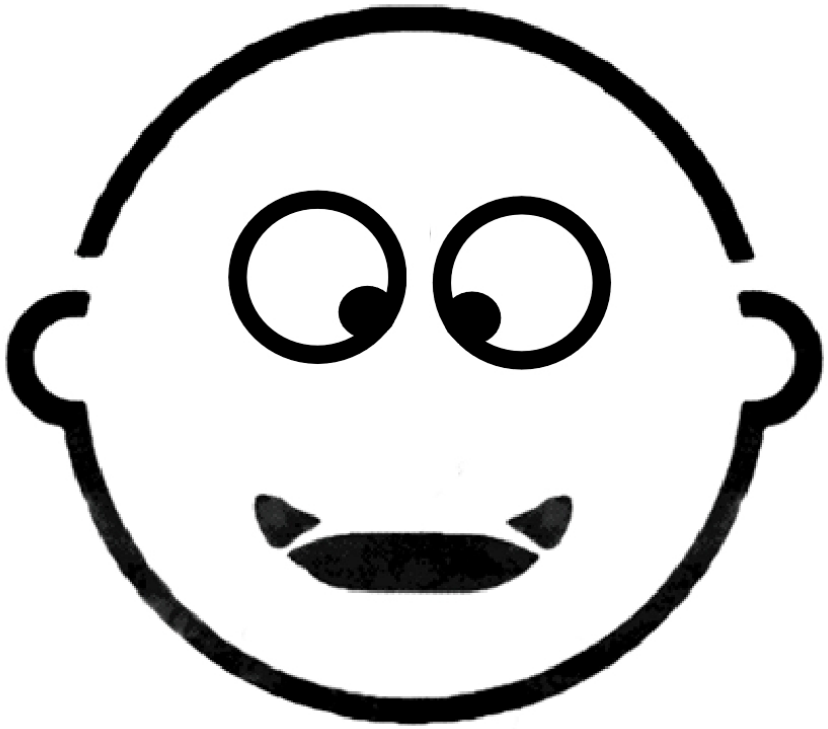
in.Security.Org
Knowledge is Security

QUESTIONS and DISCUSSION

- MANUFACTURER LIABILITY AND DUTY
- MANUFACTURER RESPONSIBILITY
- WHAT CONSTITUTES A DEFECTIVE DESIGN
- WHO SHOULD DISCLOSE
- SHOULD A SIMPLE BYPASS TECHNIQUE BE DISCOVERED BY THE MANUFACTURER
- RESPONSIBLE DISCLOSURE?

in.Security.Org
Knowledge is Security

Thank you!



Marc Weber Tobias - Matt Fiddler - Tobias Bluzmanis

©2009 Security.org

http://www.security.org

®Cliq is a registered trademark of one or more Assa Abloy Companies