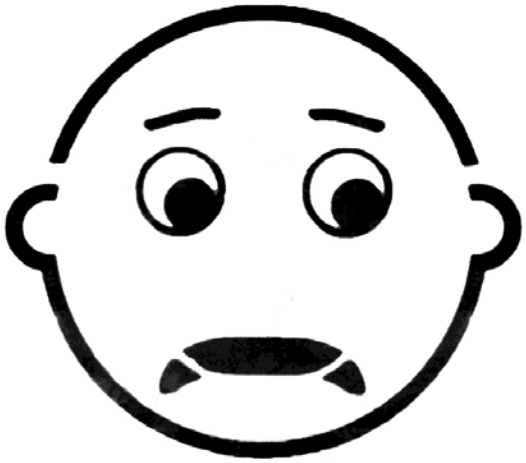
Invisible Access



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 Studies

in.Security.Org
Knowledge is Security



Standards

- 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



Standard Security Criteria

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

in.Security.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)

in.Security.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

inSecurity.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

inSecurity.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?

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

in.Security.Org
Knowledge is Security



Conventional v. High Security

- 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

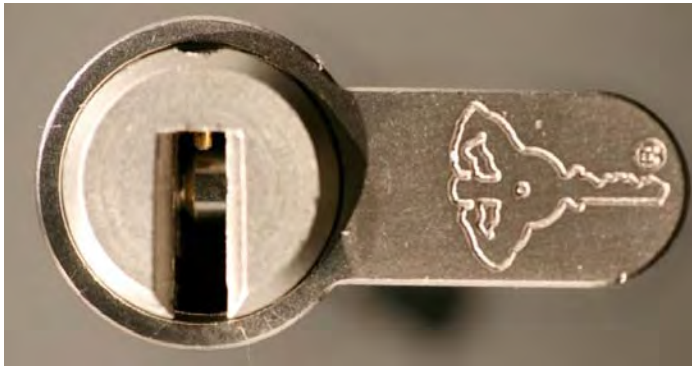
- Good for one person, one key
- No Key / User Tracking
- Addition of deletion of keys to the system
- Lost stolen or copied keys
- Manipulation of keys (Mul-T-Lock and key interchange)

in.Security.Org
Knowledge is Security



Electronic Locks: The Security Solution?





inSecurity.Org
Knowledge is Security



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



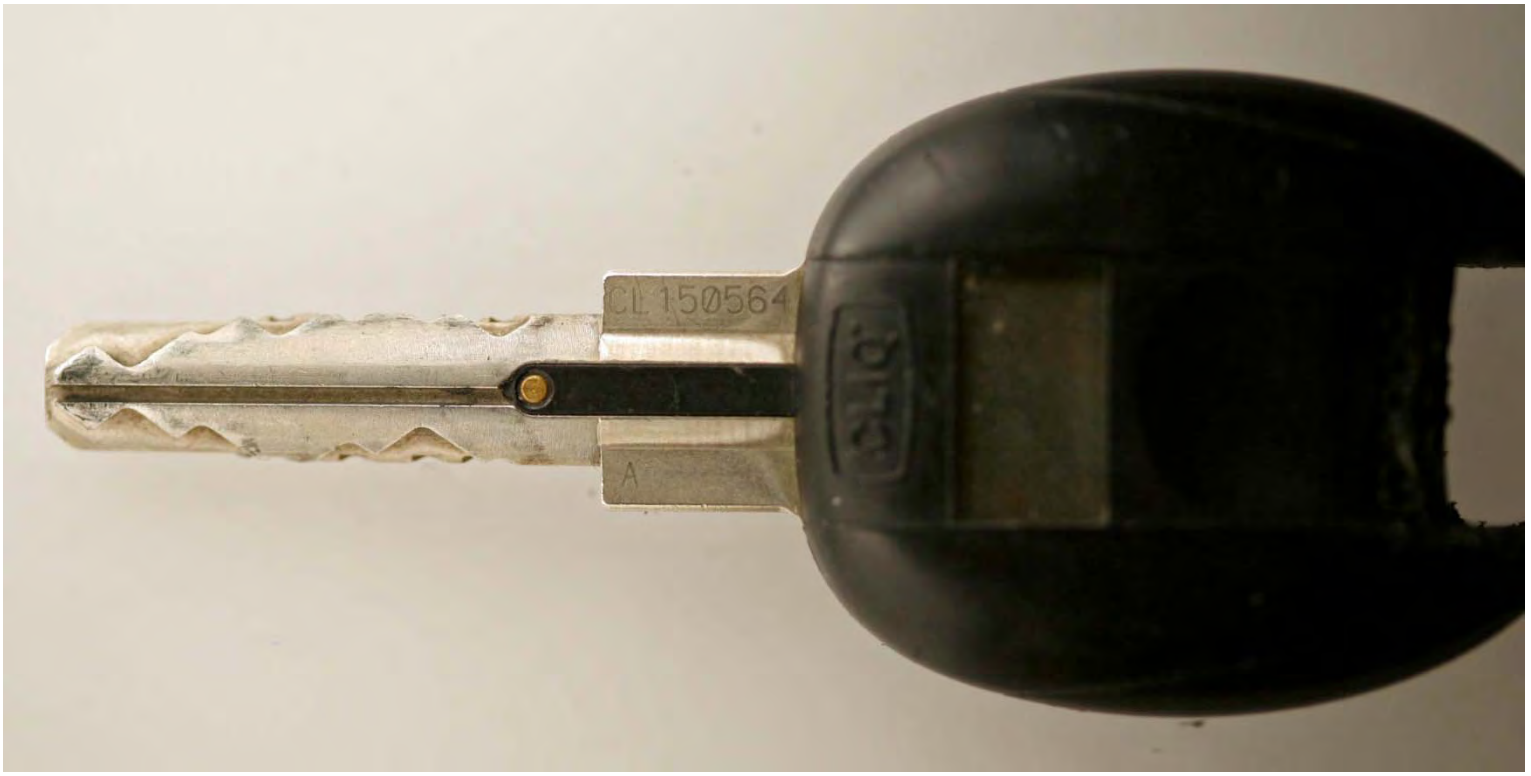
Medeco LOGIC
Higher Security?



in.Security.Org
Knowledge is Security



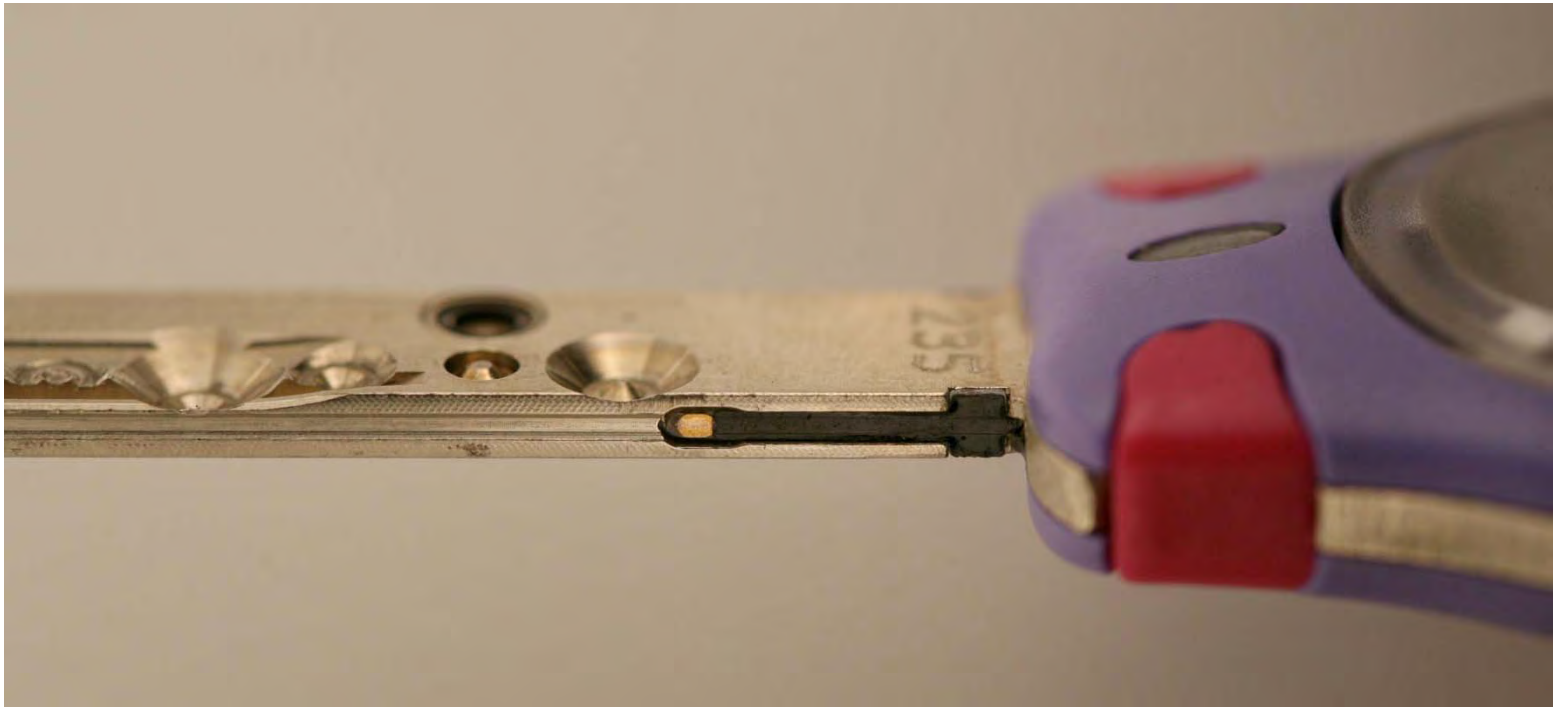
Medeco LOGIC Keys



in.Security.Org
Knowledge is Security



Mul-T-Lock Cliq: Similar Technology



in.Security.Org
Knowledge is Security



Salto and EVVA: A Different Approach





inSecurity.Org
Knowledge is Security



Critical Infrastructure

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

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

inSecurity.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



Private Aircraft Medeco Cam-Locks







in.Security.Org
Knowledge is Security



Cargo - Containers





in.Security.Org
Knowledge is Security



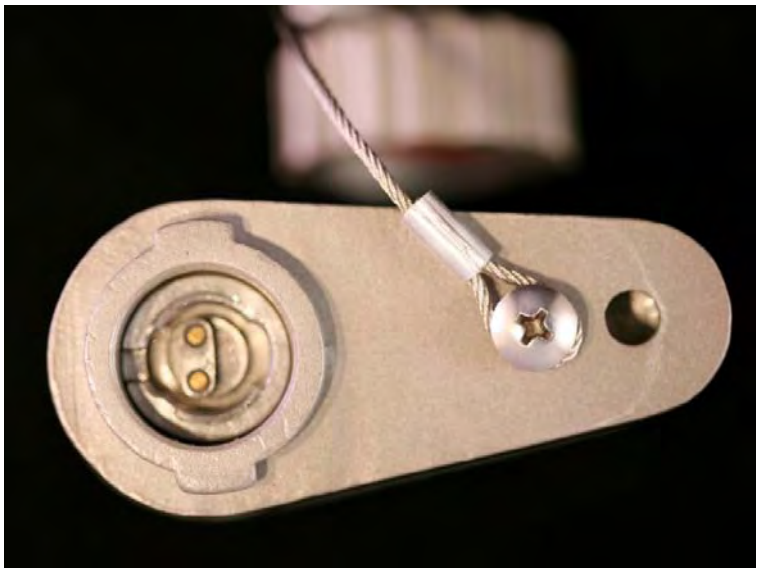
Cargo - Access

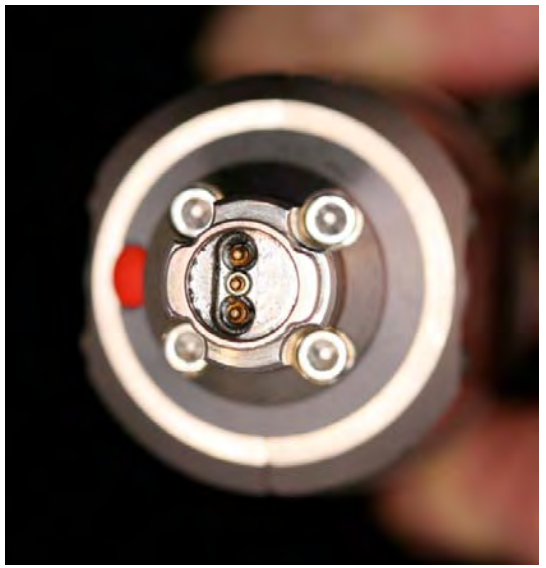
- Electronic Access Control Systems
- Electronic Padlocks with Audit Capabilities
  - Identify Tampering
  - Deter Contraband Introduction and other Attacks

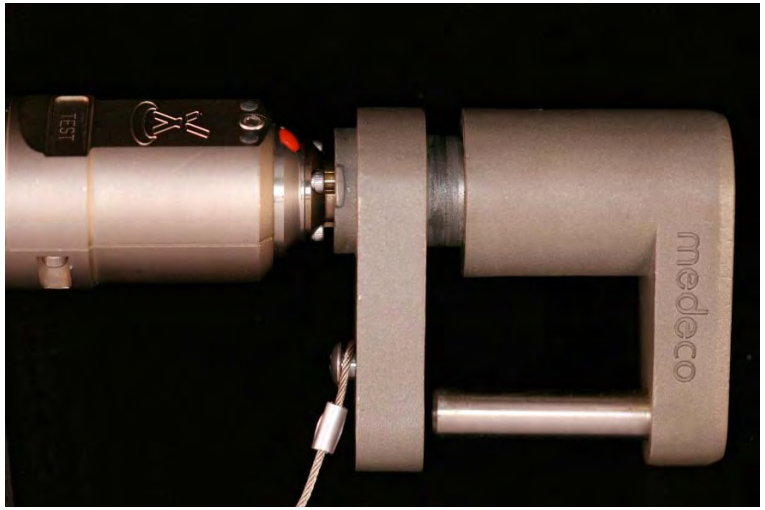
in.Security.Org
Knowledge is Security



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:

  <u>The Physical Security Plan must:</u>

"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

inSecurity.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



2008

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

in.Security.Org
Knowledge is Security















in.Security.Org
Knowledge is Security



Mechanical Locks

Not Enough Protection

- 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 Electric
    - Wired
    - Data on Card
    - Wireless

in.Security.Org
Knowledge is Security



Stand-Alone EAC

(Assa Abloy Cliq)

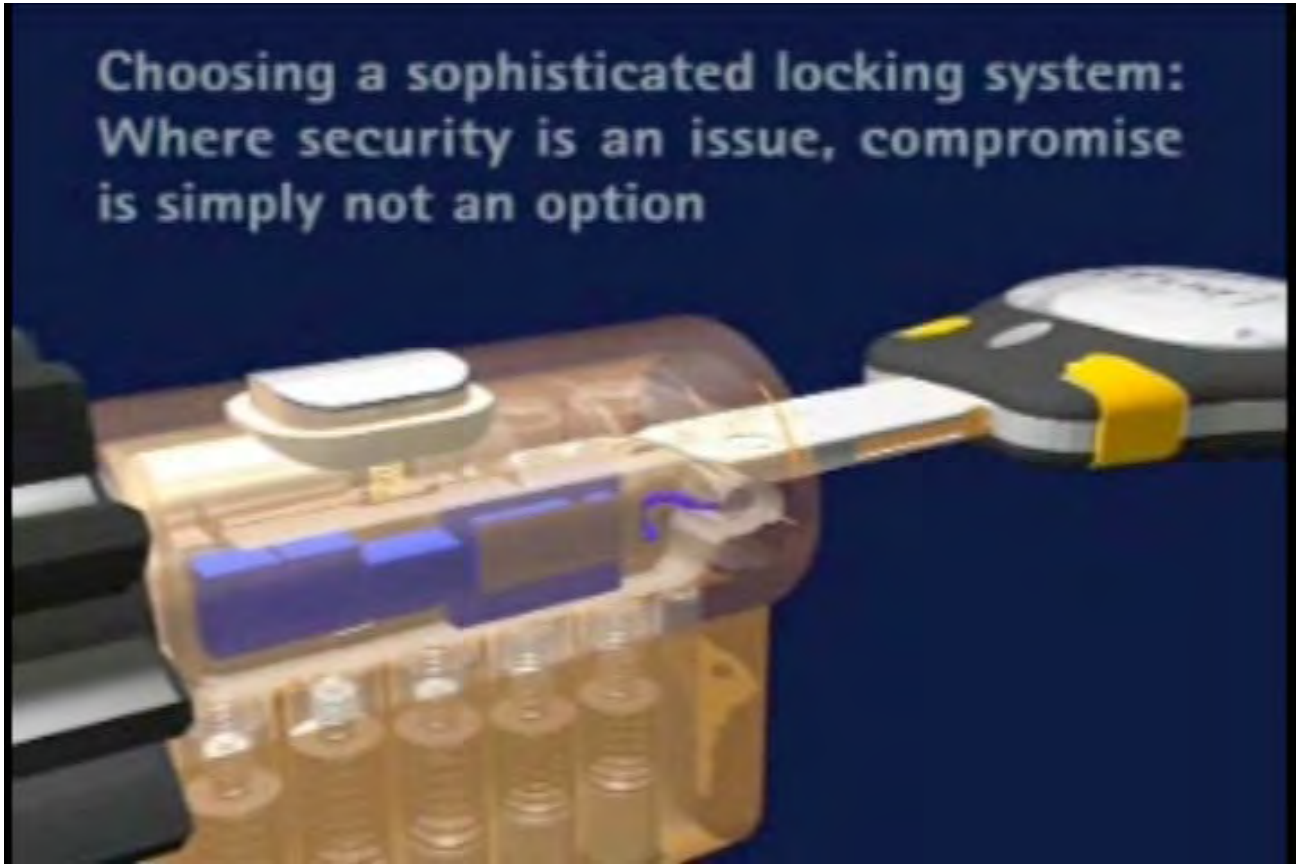
- Mul-T-Lock, Assa, Icon, Medeco Logic
  - All SAME Technology!
- Electromechanical Stand-Alone Cylinder
- Mechanical Locking + Audit
- Enhanced Control Options
- Used Throughout the World

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

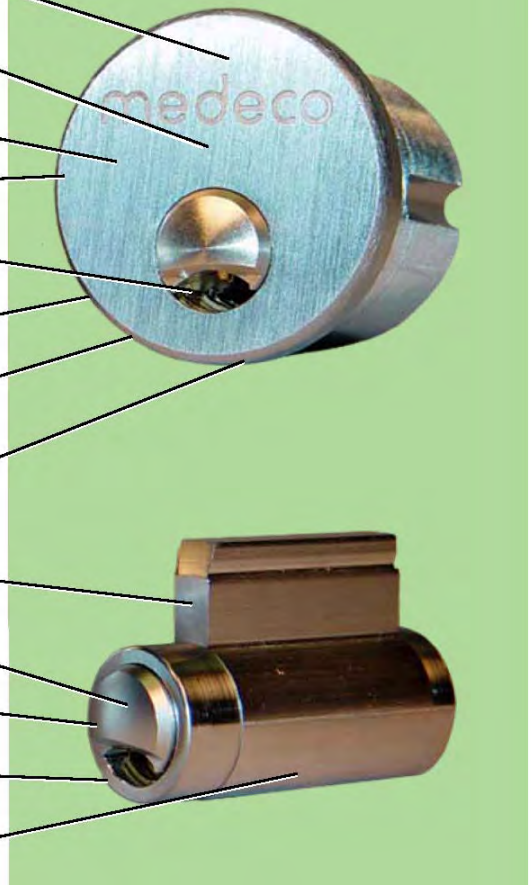
in.Security.Org
Knowledge is Security



Logic Attributes

Logic Digital Cylinder

- Program Permissions/Schedules To Either Key Or Cylinder
- Program 1,000 Authorized Keys/Groups Per Cylinder*
- Up To 750 Audit Events
- No Wiring Required
- Combines Mechanical and Electronic Security
- Fits Narrow Stile Doors
- No Additional Door Hardware Required
- No Door Hardware Modifications Required
- Easy To Maintain Power Free Cylinders
- Optional Hardened Steel Nose
- Installs In Minutes
- Available In Most Standard Finishes
- KIK, Rim, and Mortise Styles



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



Cliq and Logic Key



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 Cylinders
- Simulate Credentials
- Bypass ALL Audit Functions

in.Security.Org
Knowledge is Security



Serious Security Issues

- False Sense of Security
- 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

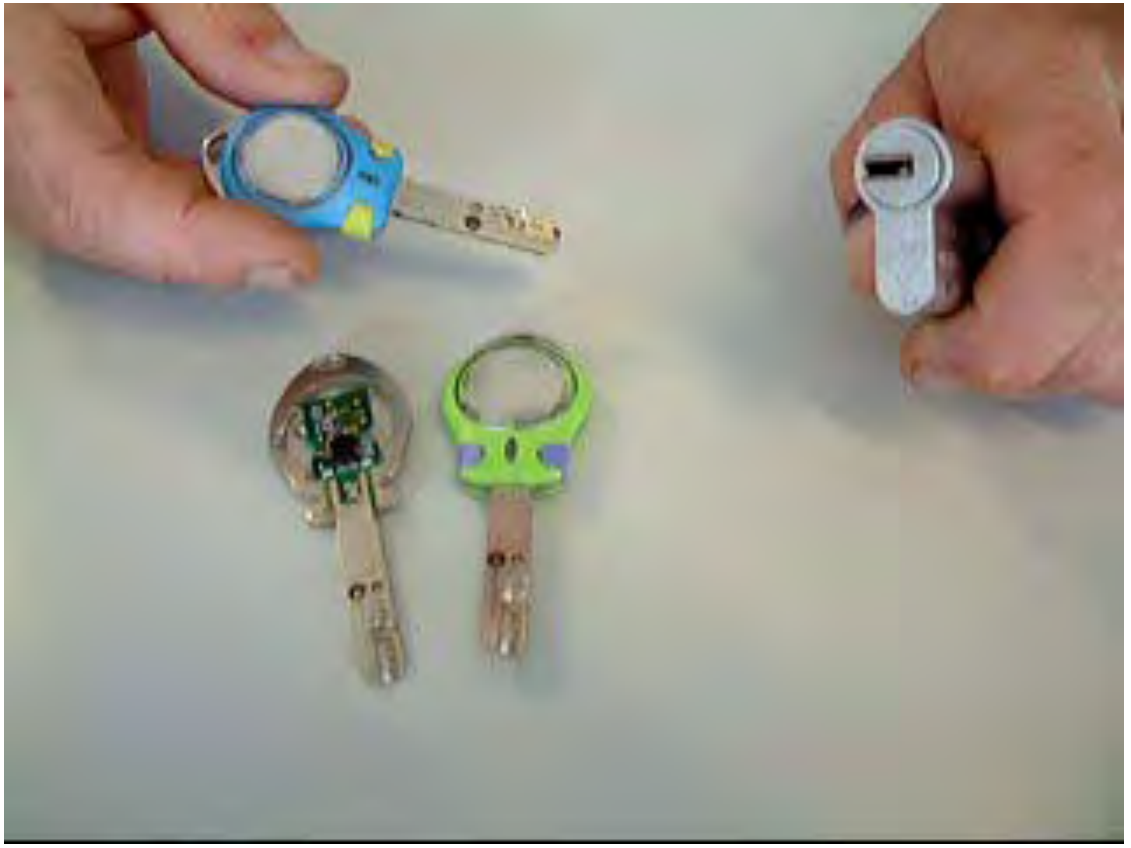
One Lost Key =

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"

inSecurity.Org
Knowledge is Security



Cliq,Logic and Nexgen Potential Issues

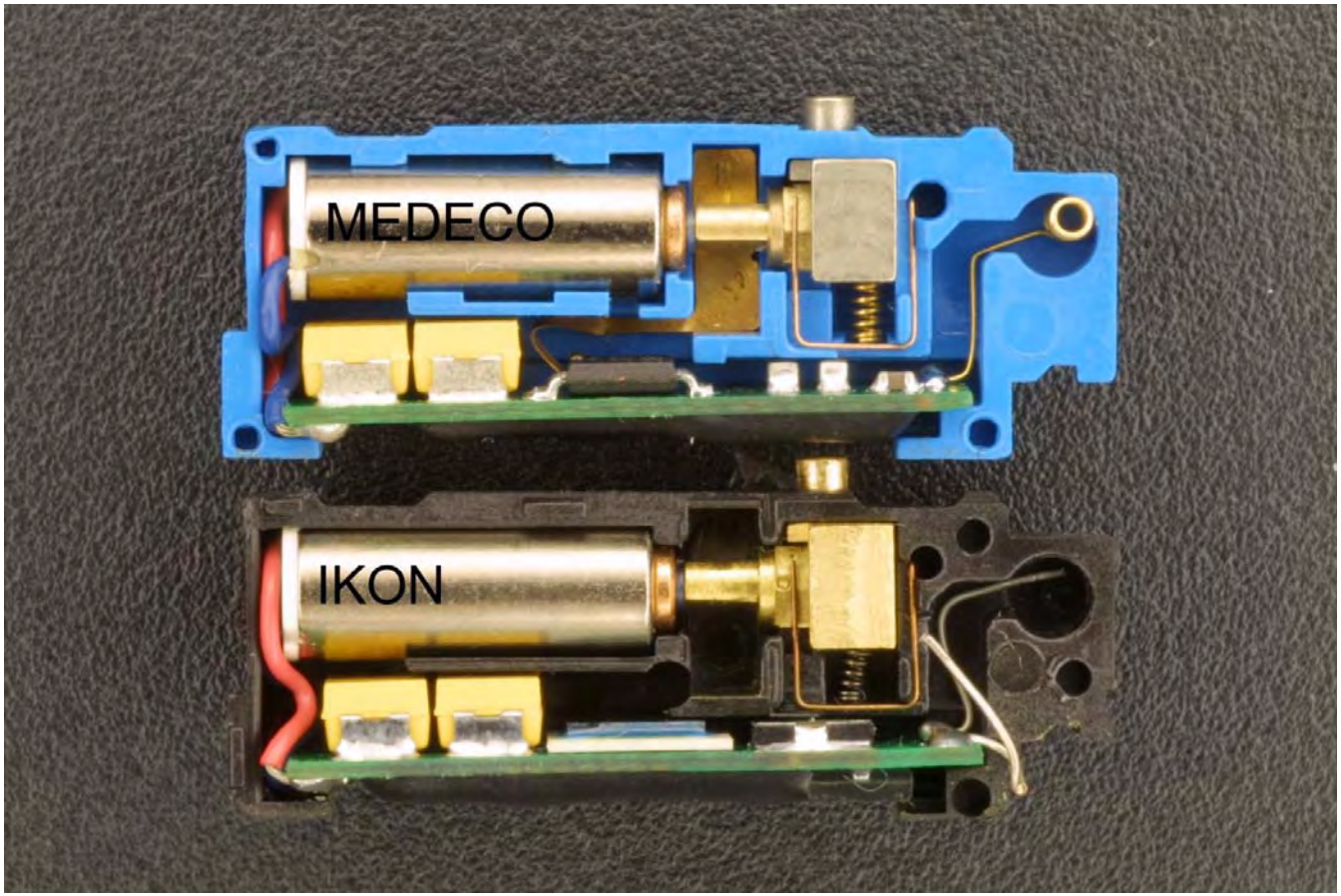
- One lost, stolen or deleted key may compromise entire system
- Simulation of Credentials
- Simulation of Keys
- Open in 30 seconds or less
- No Audit Trail

<u>Invisible Access</u>

in.Security.Org
Knowledge is Security



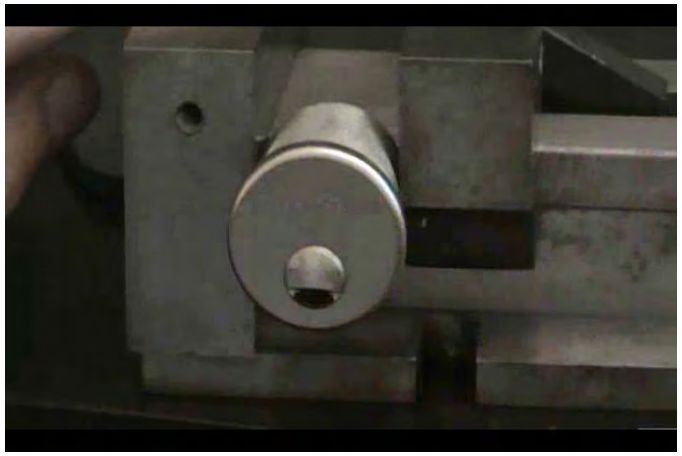
LOGIC Design



in.Security.Org
Knowledge is Security



Logic In-Security
Simulated Keys







in.Security.Org
Knowledge is Security



Logic + Cliq
Simulated Electronics



in.Security.Org
Knowledge is Security



Cliq Compromise



in.Security.Org
Knowledge is Security

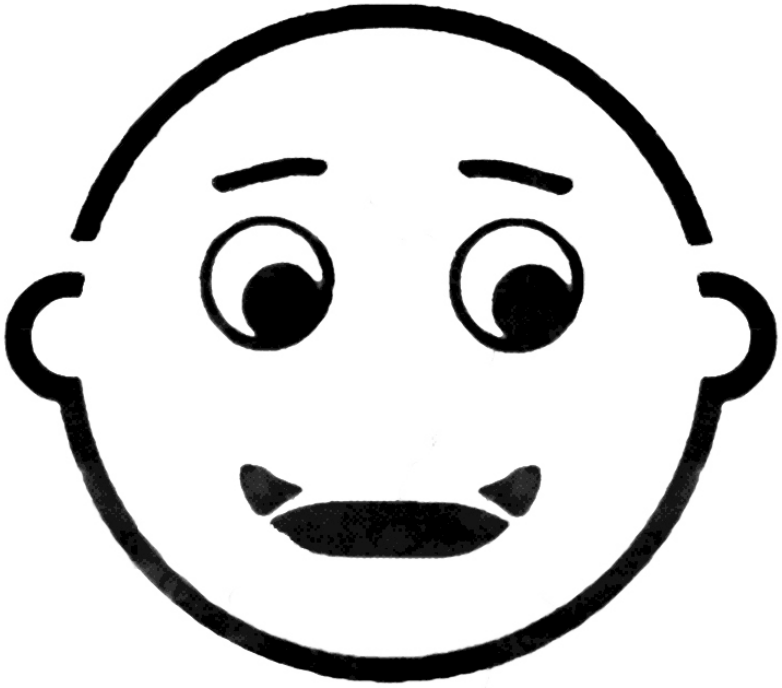


EAC-Serious Issues

- 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

Thank you!



Marc Weber Tobias - Matt Fiddler - Tobias Bluzmanis

©2009 Security.org

http://www.security.org