Ten Things You Should Know About Lockpicking

by Deviant Ollam
Event Name
XXXX-XX-XX
Who am i?
Who am I?
Who am I?

auditing
assessments
research
trainings
Who am i?

- auditing
- assessments
- research
- trainings

- workshops
- public lectures
- lockpick village
- contests & games
Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
All your hard work here...
All your hard work here... gets undermined here
Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
Pin Tumbler Locks
Pin Tumbler Locks
Pin Tumbler Locks
The View From Outside
What’s On The Inside
What’s On The Inside
It’s Not Just a Single Pin Stack
It’s Not Just a Single Pin Stack
The Key Has To Be Just Right
The Key Has To Be Just Right
Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
In An Ideal World...
In The Real World ...
In The Real World...
In The Real World...
Setting a Pin
Setting a Pin
Setting the Pins
Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement
Other Ways of Arranging the Pins
Other Ways of Attacking the Pins
A Fun Tubular Lock Story
A Fun Tubular Lock Story
Notice
This Floor may be monitored
By Closed Circuit TV
A Fun Tubular Lock Story

ROOF IS
RESTRICTED
ACCESS
Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement
5. Other everyday designs are often weak, too
Wafer Locks
Wafer Locks
Wafer Locks
Wafer Locks
Raking & Jiggling

[Images of lock mechanisms and tools]
Wafer Lock Usage
Wafer Lock Usage
Wafer Lock Usage
Wafer Lock Usage
Wafer Lock Usage
Wafer Lock Usage
Wafer Lock Usage
Wafer Lock Usage
Wafer Lock Usage
Warded Locks
Warded Locks
Warded Locks
Warded Lock Usage
Warded Lock Usage
Warded Lock Usage
Warded Lock Usage
Warded Lock Usage
Warded Lock Usage

![Warded Lock Image]

[Image: deviating.net/lockpicking]
Warded Lock Usage
Warded Lock Usage
Warded Lock Usage
Warded Lock Usage
Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement
5. Other everyday designs are often weak, too
6. You can open locks with beer and beatings
Popular Padlocks
Terrible Padlocks
Padlock Shims
Padlock Shims... From a Catalog
Padlock Shims… From a Beer Can
Padlock Shims

[Image of two padlocks with shims]
Padlock Shims
Padlock Shims
Padlock Shims
Padlock Shims
Padlock Shim Prevention

Double Ball Mechanism
Padlock Shim Prevention

Which Padlocks are Protected?
Padlock Shim Prevention

Padlock Shim Prevention
Padlock Shim Prevention

Candado doble traba a bolilla
acero inoxidable
Bumping
Bumping
Bumping
Bumping
Bumping

[Diagram of a key and lock mechanism showing the bumping technique]
Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement
5. Other everyday designs are often weak, too
6. You can open locks with beer and beatings
7. Many locks are pick resistant
Pick-Resistant Keyways
Pick-Resistant Keyways
Pick-Resistant Keyways

[Diagram of keyway]

Deviant Ollam
http://deviating.net/lockpicking
Pick-Resistant Keyways
Pick-Resistant Keyways
Pick-Resistant Pins
Pick-Resistant Pins
Pick-Resistant Pins
Pick-Resistant Pins
Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement
5. Other everyday designs are often weak, too
6. You can open locks with beer and beatings
7. Many locks are pick resistant
8. Some locks are wickedly secure
Side Bars

- Similar to side pins
- Restrict plug movement
- Harder to pick than pin stacks
Side Bars

Finger Pins
Side Bars

Finger Pins
Side Bars

Finger Pins
Schlage Primus
Side Bars

Sliders
Sliders
Side Bars

Rotating Pins
Side Bars

Rotating Pins
Rotating Pins

Medeco Locks

Medeco plug exposed, key pins rotating to align sidebar cuts

Top View          Side View
Medeco Locks
Totally shot now

- Can be picked
- Can be bumped
- Numerous weaknesses

“Open in 30 Seconds”

- Marc Tobias
- Tobias Bluzmanis
Rotating Disks

- **Tremendous Security**
  - Mimics a safe lock

- **Very Difficult To Pick**
  - Takes much time and great skill
  - Specialized tools required
Rotating Disks

- **Tremendous Security**
  - Mimics a safe lock

- **Very Difficult To Pick**
  - Takes much time and great skill
  - Specialized tools required

- **Two-in-One Tool**
  - Manipulates disks individually
  - Decodes cut positions

Barry Wels picking a rotating disk lock with Mike Glasser
Specialized Rotating Disks

- Abloy Protec
  - Not just rotating disks
  - Disk blocking mechanism
  - False cuts everywhere

- "Unpickable?"
  - Closest I ever come to using that word
  - Two-in-one tools cannot be used
Magnetic Locks

- **Miwa**
  - Japanese company
  - Array of magnetic pins
  - Simple North / South

- **Evva MCS**
  - Austrian company
  - Axial-rotated magnets
  - Interaction with sidebar
Miwa Magnetic Locks
Miwa Magnetic Locks
Miwa Magnetic Locks
Evva Magnetic Code System

- Possibly most duplication-resistant lock out there
Mul-T-Lock

External body pin
Internal body pin
Internal plug pin
External plug pin

Interactive plug pin
Interactive pin

Cylinder body
plug
No Known Attack or Bypass
Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement
5. Other everyday designs are often weak, too
6. You can open locks with beer and beatings
7. Many locks are pick resistant
8. Some locks are wickedly secure
9. It comes down to your attackers and defenders
Most Attacks are Brute Force
Social Engineering
Social Engineering

Johnny Long
Corporate Service Technician

http://deviating.net/lockpicking
Social Engineering
Social Engineering Preparedness

Stop
Social Engineering Preparedness

Stop

Challenge
Social Engineering Preparedness

Stop
Challenge
Authenticate
Social Engineering Preparedness

Stop

Challenge

Authenticate
Social Engineering Preparedness

Stop  Challenge  Authenticate

... then you follow this with “Reward”
Social Engineering
Social Engineering
Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement
5. Other everyday designs are often weak, too
6. You can open locks with beer and beatings
7. Many locks are pick resistant
8. Some locks are wickedly secure
9. It comes down to your attackers and defenders
10. The truth is out there... or, rather, in there
Forensic Evidence

[Image of a forensic officer at a crime scene]
Forensic Evidence
Forensic Evidence
Forensic Evidence – 250 uses
Forensic Evidence – 1,500 uses
Forensic Evidence - 5,000 uses
Forensic Evidence – 250 uses
Forensic Evidence – 1,500 uses
Forensic Evidence - 5,000 uses
Forensic Evidence
Forensic Evidence
Forensic Evidence

![Image of forensic evidence](http://deviating.net/lockpicking)
Forensic Evidence – picking
Forensic Evidence – raking
Forensic Evidence – both
Forensic Evidence – ugh
Forensic Evidence – wow
Forensic Evidence
Forensic Evidence - bumping
Forensic Evidence – bumping
Security is only as effective

... as the people behind it
Thank you very much.

Special thanks to TOOOL, Babak, and Daisy


this presentation is CopyLeft by Deviant Ollam. you are free to reuse any or all of this material as long as it is attributed and freedom for other s to do the same is maintained