

[ccc-tv](#)



- [C3TV - News](#)
- [C3TV - RSS, last 100](#)
- [C3TV - Podcast feed of the last two years](#)
- [C3TV - Podcast audio feed of the last year](#)
- [C3TV - Podcast archive feed, everything older than two years](#)
-

-
- Podcast feeds for 32c3

- [mp4](#)
- [webm](#)
- [WEBM \(HD\)](#)
- [MP3](#)
- [opus](#)
- [MP4 \(html5\)](#)
- [MP4 \(HD\)](#)



1. [browse](#)
2. [congress](#)
3. [2015](#)
4. event

Reversing UEFI by execution

[Jethro Beekman](#)

- [Video](#)
- [Download](#)
- [Share](#)

Video Player

How Lenovo turns 64 chars into 32 bytes

$AtaPassword \leftarrow \text{SHA}_{256}(\text{SHA}_{256}(Password) \parallel AtaIdentity_{SerialNumber} \parallel AtaIdentity_{ModelNumber})$

actually:

$PasswordHash \leftarrow \text{SHA}_{256}((\text{ToScanCodes}(\text{LowerCase}(Password)) \parallel \text{"\textbackslash"}^{64})_{1:64})_{1:12}$

$SN \leftarrow AtaIdentity_{SerialNumber} \quad MN \leftarrow AtaIdentity_{ModelNumber}$

$AtaPassword \leftarrow \text{SHA}_{256}(PasswordHash \parallel \text{SwapBytes}(SN) \parallel \text{SwapBytes}(MN))$

32C3 - Jethro Beekman

max 96 bits of entropy!



GATED COMMUNITIES

- MP4 (HD) en-de [http download torrent](http://download.torrent)

How Lenovo turns 64 chars into 32 bytes

parent directory

congress/2015

embed into your website

actually:

max 96 bits of entropy!

<iframe width="853" height="480" src="https://media.ccc.de/v/32c3-7245-reversing_uefi_by_e"

$PasswordHash \leftarrow \text{SHA}_{256}((\text{ToScanCodes}(\text{LowerCase}(Password)) \parallel \text{"\textbackslash"}^{64})_{1:64})_{1:12}$

$SN \leftarrow AtaIdentity_{SerialNumber} \quad MN \leftarrow AtaIdentity_{ModelNumber}$

$AtaPassword \leftarrow \text{SHA}_{256}(PasswordHash \parallel \text{SwapBytes}(SN) \parallel \text{SwapBytes}(MN))$

32C3 - Jethro Beekman

- [via Twitter](#)
- [via Facebook](#)
- [via Google+](#)
- [via App.net](#)
- [by Mail](#)



GATED COMMUNITIES

- 24 min
- 2015-12-29
- 514
- streaming.media.ccc.de

About

This talk will be an overview of how to reverse-engineer Unified Extensible Firmware Interface (UEFI) firmware, the replacement for BIOS. Various useful tools will be discussed, including those written by the presenter and those written by others. One of the highlights will be a tool that enables running parts of the firmware in userspace on a standard Operating System.

Tags

[Security](#)
by [Chaos Computer Club e.V](#)