


Utilman is back

Bypassing BitLocker and Windows Logon with DMA

 **Bundesministerium**
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie

 **Bundesministerium**
Digitalisierung und
Wirtschaftsstandort



FWF
Der Wissenschaftsfonds.



A Little Bit of History

The screenshot shows a web browser window displaying the search results for 'shellcode' on the milw0rm website. The page features a dark theme with green text and a 'MILWORM' logo at the top. A search bar is visible with the text 'Search:' and a 'Submit' button. Below the search bar, there are three sections of results: 'exploits/shellcode', 'papers', and 'videos'. Each section contains a table with columns for date, description, hits, and author. The 'exploits/shellcode' section lists various exploits such as 'TIPTEST 3.1.7 Stack Buffer Overflow PoC' and 'Active Feed 2.1 (Gmail) Blind SQL Injection Vulnerability'. The 'papers' section includes 'Exploiting Tomcat's Internal Today: Penetration Testing with IPv6' and 'Auditing mailing scripts for web app penetration'. The 'videos' section features 'MS09-052 exploit (E7) Exposed Opening LAN for Penetration'.

milw0rm - exploits : vulnerabilities : videos : papers : shellcode - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.milw0rm.com/search.php?

[home] [contents] [platforms] [shellcode] [search] [cracker] [links] [rss] [archive]

MILWORM

Search: Submit

[exploits/shellcode]

DATE	DESCRIPTION	HITS	AUTHOR
2006-02-16	TIPTEST 3.1.7 Stack Buffer Overflow PoC	1728	Fred
2006-11-20	Active Feed 2.1 (Gmail) Blind SQL Injection Vulnerability	923	Rid-Dyck
2006-11-20	Active Feed 2.1 (Auth System) Remote SQL Injection Vulnerability	964	Rid-Dyck
2006-09-01	Living Local Website (DotTest.php) SQL Injection Vulnerability	2299	Hooze X
2006-07-25	phpTest 6.6.3 (joomla.php image_id) Remote SQL Injection Vulnerability	2208	cOndemned
2006-04-19	Apartment Search Script (DotTest.php) SQL Injection Vulnerability	3423	Crackers_Child
2006-02-07	infocommerce Admin Customer Testimonials 3.1 SQL Injection Vulnerability	13093	it's my
2006-01-29	Genetic Analysis 2.0 (Executive) Remote Command Execution Exploit	5568	W X
2004-04-07	FrontPage Backlog 2.1 (Default) Buffer Overflow Exploit	4166	1st 488
2003-09-21	hotty 2.0 Local root exploit (Tested on Red Hat 9.0)	4306	chobby
2003-09-16	MS03-09-16: MSN Stress Tester Denial of Service Exploit	4627	Cps
2001-01-15	Seppit Exploit / Tested Version 2.1 rev. 46 (MSB Linux)	2533	teletiter

[papers]

DATE	DESCRIPTION	HITS	AUTHOR
2006-10-13	Exploiting Tomcat's Internal Today: Penetration Testing with IPv6	2511	H D Mouse
2006-07-15	Auditing mailing scripts for web app penetration	2792	Adrian "pegasus" Plaster
2007-04-18	Buffer Overflow testing on postfix gcc 4.3.3	7164	swings
2006-11-13	Vulnerability Enumeration For Penetration Testing	12280	Alphabatic Mangarok

[videos]

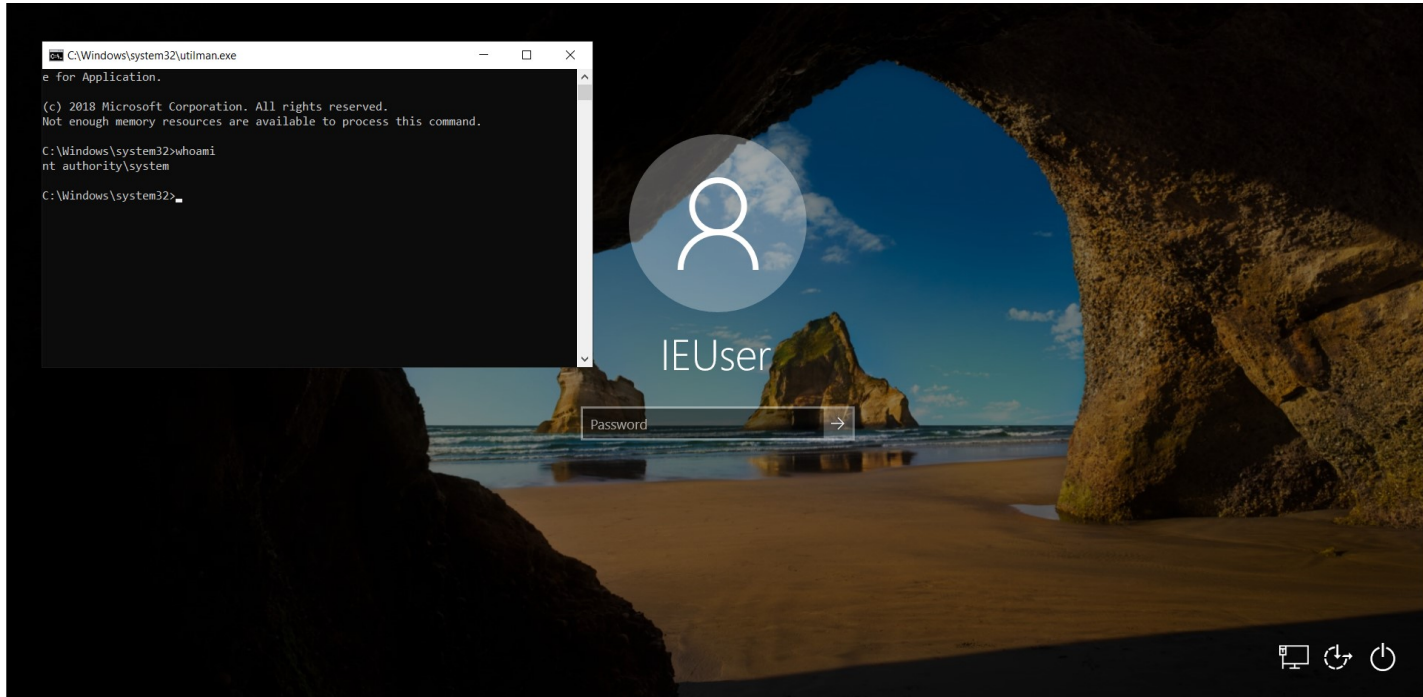
DATE	DESCRIPTION	HITS	AUTHOR
2009-03-12	MS09-052 exploit (E7) Exposed Opening LAN for Penetration	13705	WirelessPunkin

[author]

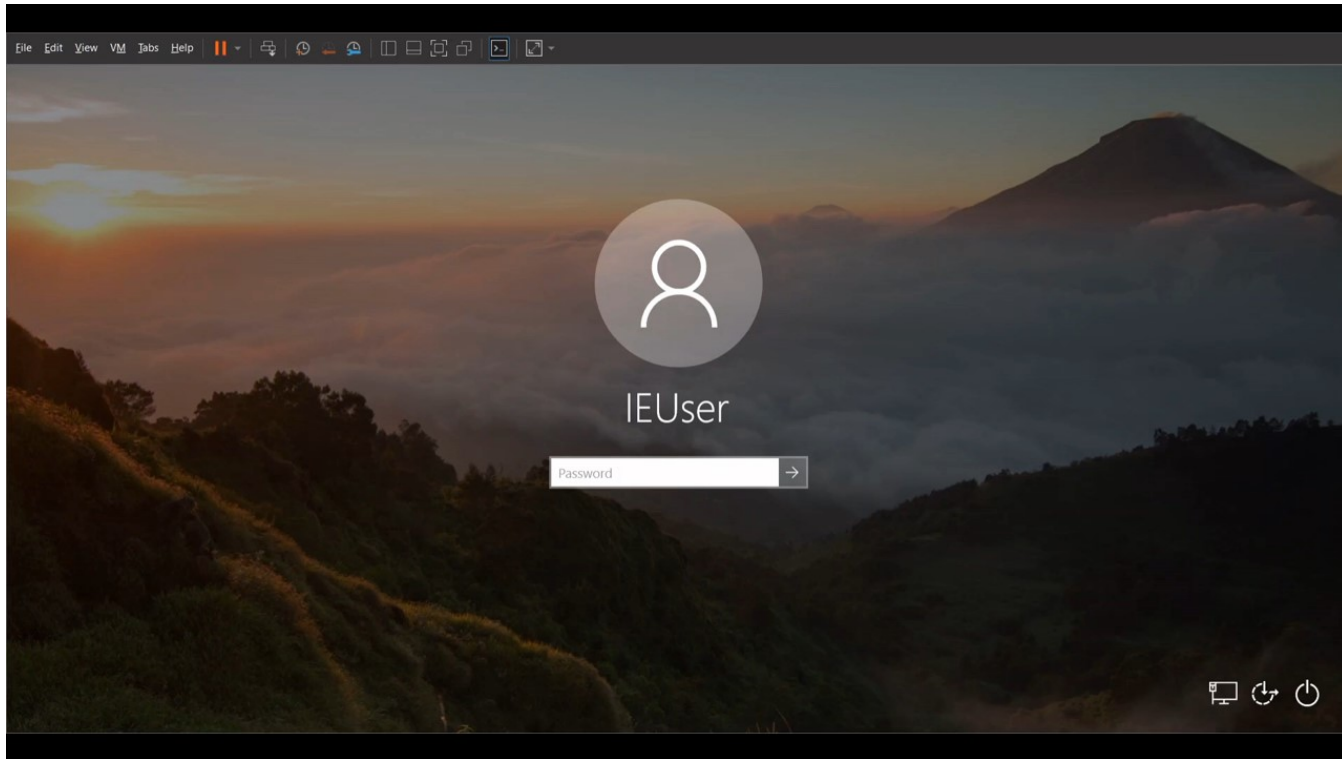
Author: gtm01
Site: RedTeam PenTesting - http://redteam-pentesting.de

Done

A Little Bit of History



How Does This Work? (Video-Demo)



<https://youtu.be/A565BO0p5Yw>

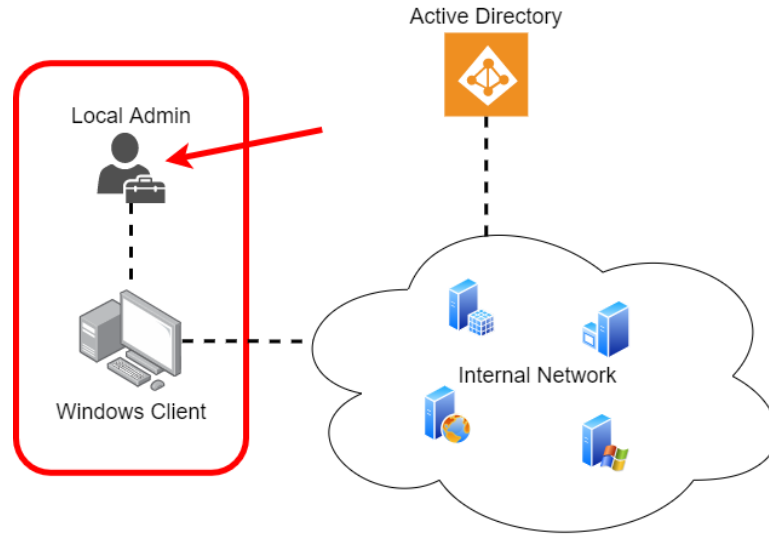
whoami /all

Martin Grottenthaler @ SBA Research

Penetration testing of Windows clients, internal networks and Active Directory

Domain Admin in **your** Active Directory (?)

Today's Scope



BitLocker Killed Our Exploit 🥲

We cannot modify data on encrypted drives

What if we know the BitLocker PIN or there is none?

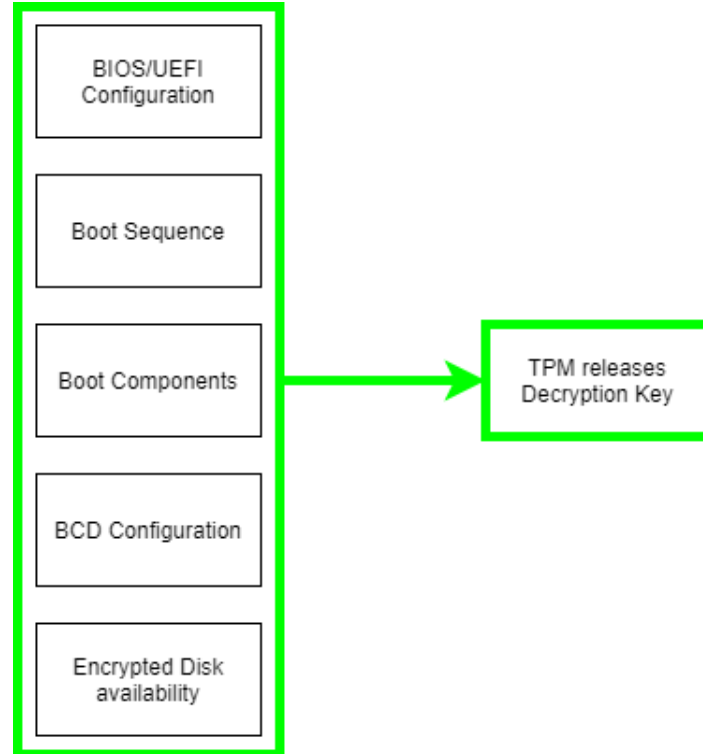
TPM (Trusted Platform Module)

Special hardware for cryptographic operations

Stores and protects our BitLocker key

and only releases it if the boot process is unaltered

Boot Process Security



The Check Fails

BitLocker recovery

Enter the recovery key for this drive

Use the number keys or function keys F1-F10 (use F10 for 0).

Recovery key ID (to identify your key): ABD09F3E-C04C-4C8F-B2AE-CF0253006F7B

Here's how to find your key:

- Sign in on another device and go to: <http://custom.url.contoso.com>
- Try your Microsoft account at: aka.ms/myrecoverykey
- For more information go to: aka.ms/recoverykeyfaq

BitLocker Modes

The good – TPM and PIN

The bad and default – TPM only

and the ugly – without TPM (better than nothing)

TPM and PIN

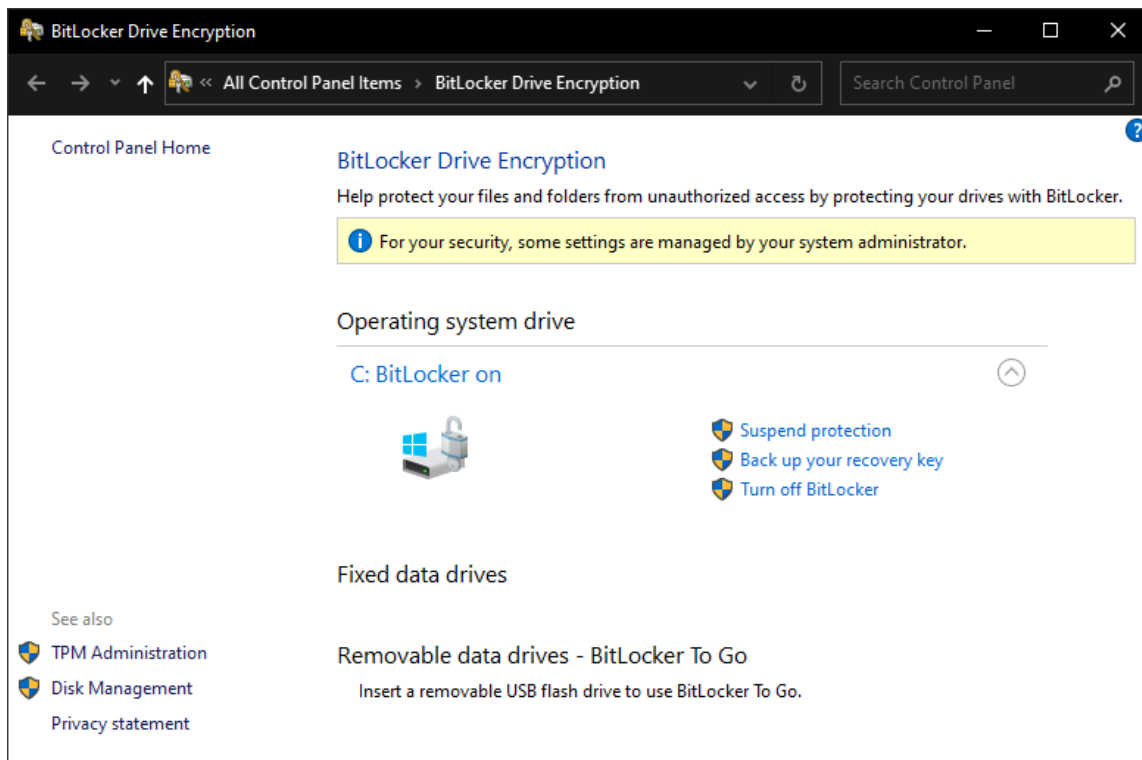
BitLocker

Enter the PIN to unlock this drive

Use the number keys or function keys F1-F10 (use F10 for 0).

Press the Insert key to see the PIN as you type.

TPM only



The screenshot shows the Windows BitLocker Drive Encryption control panel window. The title bar reads "BitLocker Drive Encryption". The navigation bar includes "All Control Panel Items" and "BitLocker Drive Encryption". A search box is present on the right. The main content area is titled "BitLocker Drive Encryption" and includes a help link. A yellow information banner states: "For your security, some settings are managed by your system administrator." Below this, the "Operating system drive" section shows "C: BitLocker on" with a lock icon and three options: "Suspend protection", "Back up your recovery key", and "Turn off BitLocker". The "Fixed data drives" section is currently empty. The "Removable data drives - BitLocker To Go" section includes the instruction: "Insert a removable USB flash drive to use BitLocker To Go." A "See also" section on the left lists "TPM Administration", "Disk Management", and "Privacy statement".

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

i For your security, some settings are managed by your system administrator.

Operating system drive

C: BitLocker on

- Suspend protection
- Back up your recovery key
- Turn off BitLocker

Fixed data drives

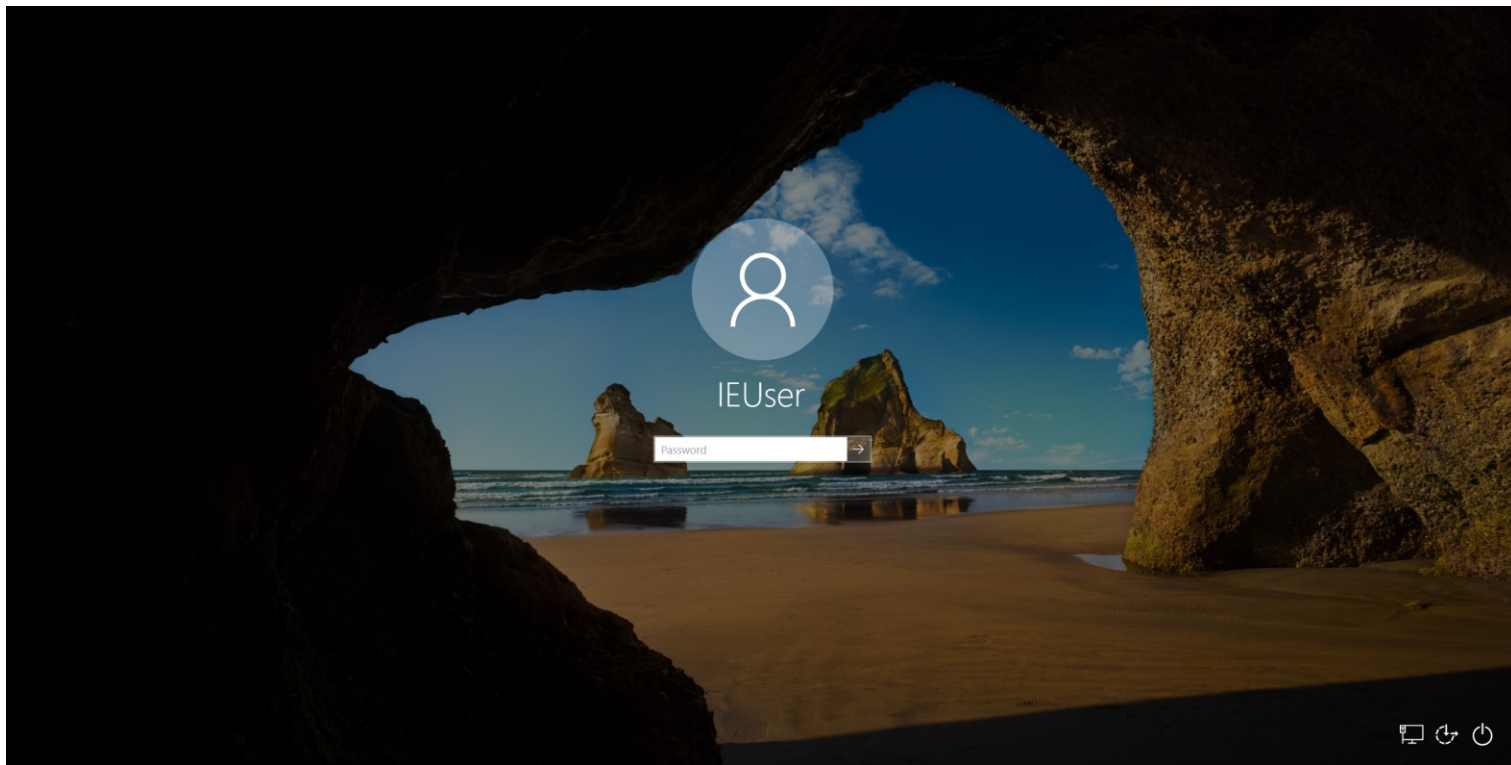
See also

- TPM Administration
- Disk Management
- Privacy statement

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

TPM only



Where Can We Attack?

Let's just attack the Windows logon!

And I am not talking about brute force attacks

DMA (Direct Memory Access)

Allows hardware to access RAM independently of the CPU

Your graphics card uses this!

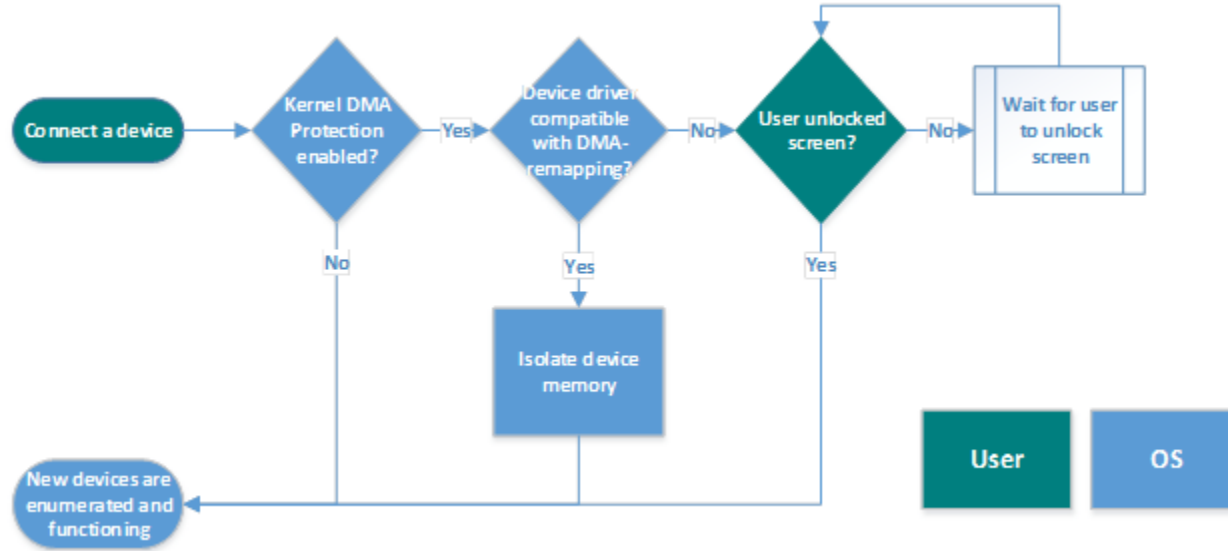
Does Anybody Remember This?



What's This New Thing?



Kernel DMA Protection



There Is Another Way

PCI Express also allows Direct Memory Access

And most devices have PCIe (maybe over M.2)

Let's Try It Out! (Live-Demo)

We will have to do some work



What Is Vulnerable?

- Full volume encryption without pre-boot authentication
- Full volume encryption **with** pre-boot authentication **if the PIN is known to the attacker**

Countermeasures

Pre-boot authentication (BitLocker PIN)

Protects against thieves

Does not protect against local privilege escalation
by a legitimate user

Additional Countermeasures

- Virtualization Based Security
- Kernel DMA Protection

These need hardware support! (and correct BitLocker configuration)

Key Takeaways (1/2)

- Use pre-boot authentication to protect against outside attackers
 - Also protects against attacks on TPM

Key Takeaways (2/2)

- Do not assume that local privilege escalation is impossible (see various other vulnerabilities)
- **Secure your Active Directory!** This is where your crown jewels are!


Martin Grottenthaler

SBA Research

Floragasse 7, 1040 Vienna

+43 664 881 040 84

mgrottenthaler@sba-research.org

 Bundesministerium
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie

 Bundesministerium
Digitalisierung und
Wirtschaftsstandort



wirtschafts
agentur
wien
Ein Fonds der
Stadt Wien



FWF
Der Wissenschaftsfonds.

 netidee
OPEN INNOVATIONS

Further Information

1. Utilman Attack Video: <https://youtu.be/A565BO0p5Yw>
2. Utilman Attack Explained: <http://index-of.es/Exploit/EN-Bypass%20windows%20server%202008.pdf>
3. BitLocker Countermeasures: <https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-countermeasures>
4. Virtualization based security: <https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-vbs>
5. TPM platform validation profiles:
https://admx.help/?Category=MDOP&Policy=Microsoft.Policies.BitLockerManagement::PlatformValidation_UEFI_Name
6. PCILeech: <https://github.com/ufrisk/pcileech>
7. TPM-Fail Attack: <https://tpm.fail/>
8. This attack shown by somebody else: <https://www.synacktiv.com/en/publications/practical-dma-attack-on-windows-10.html>