

A vertical decorative strip on the left side of the slide, showing a close-up of a computer keyboard with a yellow padlock resting on one of the keys.

Crypto-based security mechanisms in Windows and .NET

A summary of Alexandre Herzog's
MAS in Information Security 18 Thesis

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Agenda



Introduction

Work content and methodology

Phase 1 - Security mechanism overview

Phase 2 - In-depth analysis and findings

Recommendations & What's new since its release?

Conclusion

Questions

Introduction

Work content and methodology

Phase 1 - Security mechanism overview

Phase 2 - In-depth analysis and findings

Recommendations & What's new since its release?

Conclusion

Questions

Never so much data has been generated and had to be protected

Cryptography is now ubiquitous in our daily life

Crypto helps not only to protect confidentiality but can also guarantee

- ✦ Integrity
- ✦ Authenticity
- ✦ Non-repudiation
- ✦ Liability

«The aim of this work is to provide an exhaustive overview of crypto-based security mechanisms implemented in Windows and in the .NET framework»



Vaudois exilé d'abord en Valais, then Wellington (NZ) und jetzt Zürich

Mainly worked for banks as sysadmin / developer

Recently finished my MAS in Information Security at HSLU

Author of several security advisory

- ✦ Including CVE-2013-1330 patched in MS13-067 (SharePoint), MS13-105 (Outlook Web Access) and probably related to other fixes (e.g. MS13-100, KB2905247 ? ;-)

Invited by Microsoft to BlueHat back in December 2013

Since 01.01.2014 CTO of Compass Security Schweiz AG

Introduction – About the work



Main scope of the thesis was Windows 7

- ✦ Windows 8 was not yet seen as enterprise ready
- ✦ Windows 8.1 just came out as preview

Indirectly got me invited to Seattle in December 2013

Won the SGRP 1337 award in 2013



SGRP 1337 Preis - Durchführungen [Bedingungen]

| Jahr | Informationen | Einsendeschluss |
|--------|--|-----------------|
| • 2013 | Der Masterarbeit "Crypto-based security mechanisms in Windows and .NET" von Alexandre Herzog wird mit dem SGRP Preis 1337 ausgezeichnet - Herzliche Gratulation! | - |
| • 2014 | Bewerbungen für den SGRP 1337 Preis 2014 werden ab sofort entgegengenommen. Die Bedingungen für den SGRP 1337 Preis sind zu beachten. Das Bewerbungsdossier muss bis am 15. Oktober 2014 per E-Mail an den Präsidenten der SGRP eingereicht werde. | 15.10.2014 |

Agenda



Introduction

Work content and methodology

Phase 1 - Security mechanism overview

Phase 2 - In-depth analysis and findings

Recommendations & What's new since its release?

Conclusion

Questions

Work was divided into 2 phases:

First phase included

- ✦ Establishing a list of security mechanisms which may rely on cryptographic operations
- ✦ Investigating each security mechanism
- ✦ Documenting the security mechanism and identify dependencies
- ✦ Rating the importance of the security mechanism

Second phase focused on specific aspects of 3 security mechanisms

- ✦ In scope were the top 3 mechanisms identified by the earlier performed rating
- ✦ Performed activities varied for each mechanism
 - ✦ Performing attack A with tool T on crypto based security mechanism X
 - ✦ Audit and exploitation of mechanism Y
 - ✦ Study of new feature Z

Agenda



Introduction

Work content and methodology

Phase 1 - Security mechanism overview

Phase 2 - In-depth analysis and findings

Recommendations & What's new since its release?

Conclusion

Questions

Phase 1 - Security mechanism overview



List of security mechanisms

- ✦ Initially included 15 security mechanisms
- ✦ 12 of these 15 rely on cryptography

Investigating each security mechanism

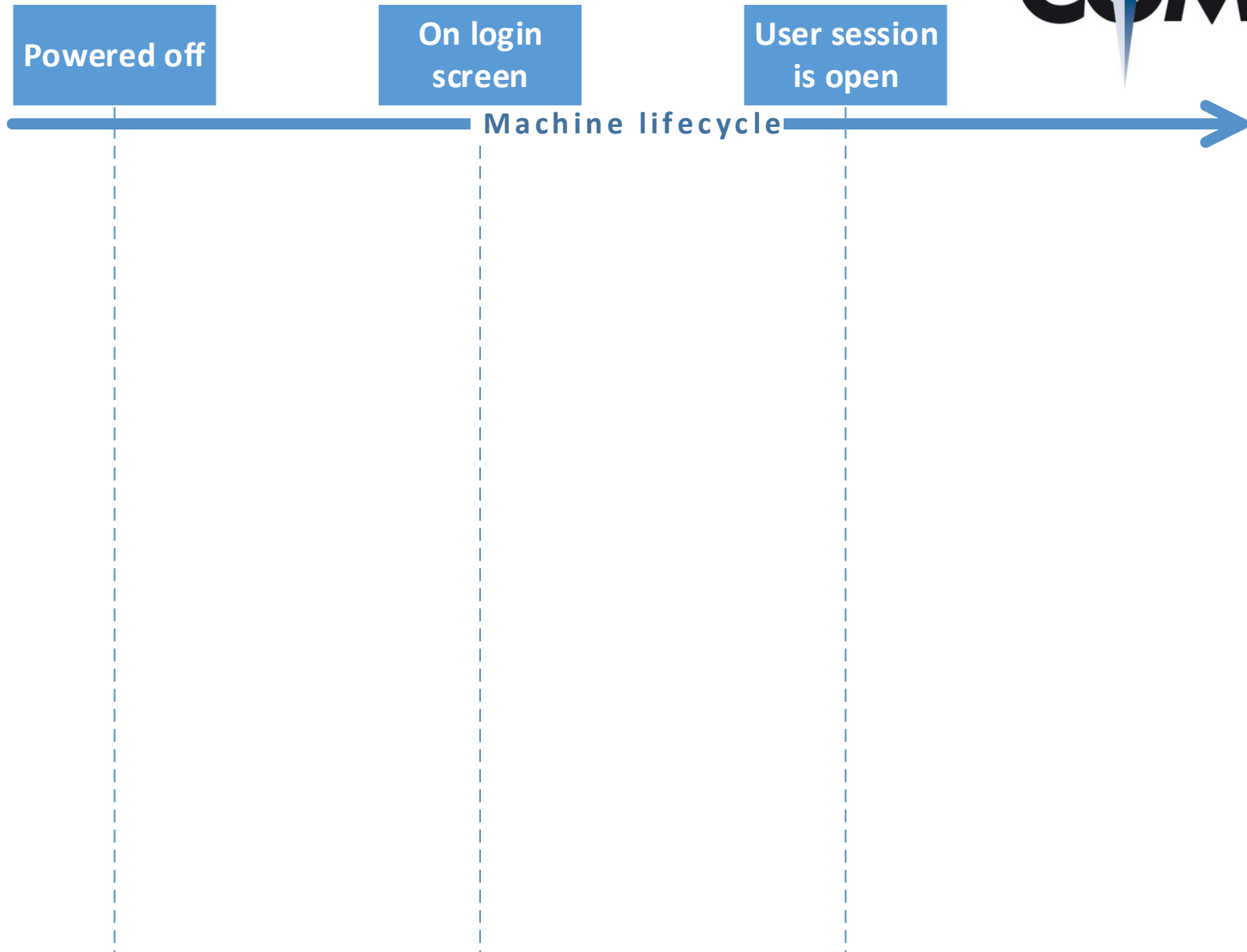
- ✦ Introduction chapter
- ✦ Overview table including dependencies
- ✦ Relevant documentation and open points
- ✦ Current attack and tools
- ✦ Countermeasures and recommendations

Outcome useful for

- ✦ Anyone involved with Microsoft technologies
- ✦ Security officers to understand threats
- ✦ Security consultants and/or researchers as a starting point for further investigations

- 2 List of security mechanisms
 - 2.1 Introduction, methodology and scope
 - 2.1.1 Windows SysKey/BootKey
 - 2.2 Windows SysKey/BootKey
 - 2.2.1 Encrypting File System (EFS)
 - 2.2.1.1 Introduction
 - 2.2.1.2 Relevant documentation and open points
 - 2.2.1.3 Current attacks and tools
 - 2.2.1.3.1 Recovery of the BootKey
 - 2.2.1.3.2 Cold Boot / FireWire / Thunderbolt / Direct Memory Access
 - 2.2.1.3.3 Evil Maid attack
 - 2.2.1.3.4 Password brute force
 - 2.2.1.4 Countermeasures and recommendations
 - 2.2.2 Encrypted File System (EFS)
 - 2.2.2.1 Introduction
 - 2.2.2.2 Relevant documentation and open points
 - 2.2.2.3 Current attacks and tools
 - 2.2.2.3.1 Recovery of temporary files
 - 2.2.2.3.2 Abuse of file synchronisation / offline file sync
 - 2.2.2.3.3 Cold Boot / FireWire / Thunderbolt / Direct Memory Access
 - 2.2.2.3.4 Evil Maid attack
 - 2.2.2.4 Countermeasures and recommendations
 - 2.3 Encrypted File System (EFS)
 - 2.3.1 Introduction
 - 2.3.2 Relevant documentation and open points
 - 2.3.3 Current attacks and tools
 - 2.3.3.1 Recovery of temporary files
 - 2.3.3.2 Abuse of file synchronisation / offline file sync
 - 2.3.3.3 Cold Boot / FireWire / Thunderbolt / Direct Memory Access
 - 2.3.3.4 Evil Maid attack
 - 2.3.4 Countermeasures and recommendations

Phase 1 - Security mechanism overview



Windows SysKey/BootKey

- ✦ Security feature introduced in 1997 against SAM attacks
- ✦ Legacy encryption mechanism which got bypassed in 2004
- ✦ Still possible to protect your Windows 8.1 SAM with a boot-time password

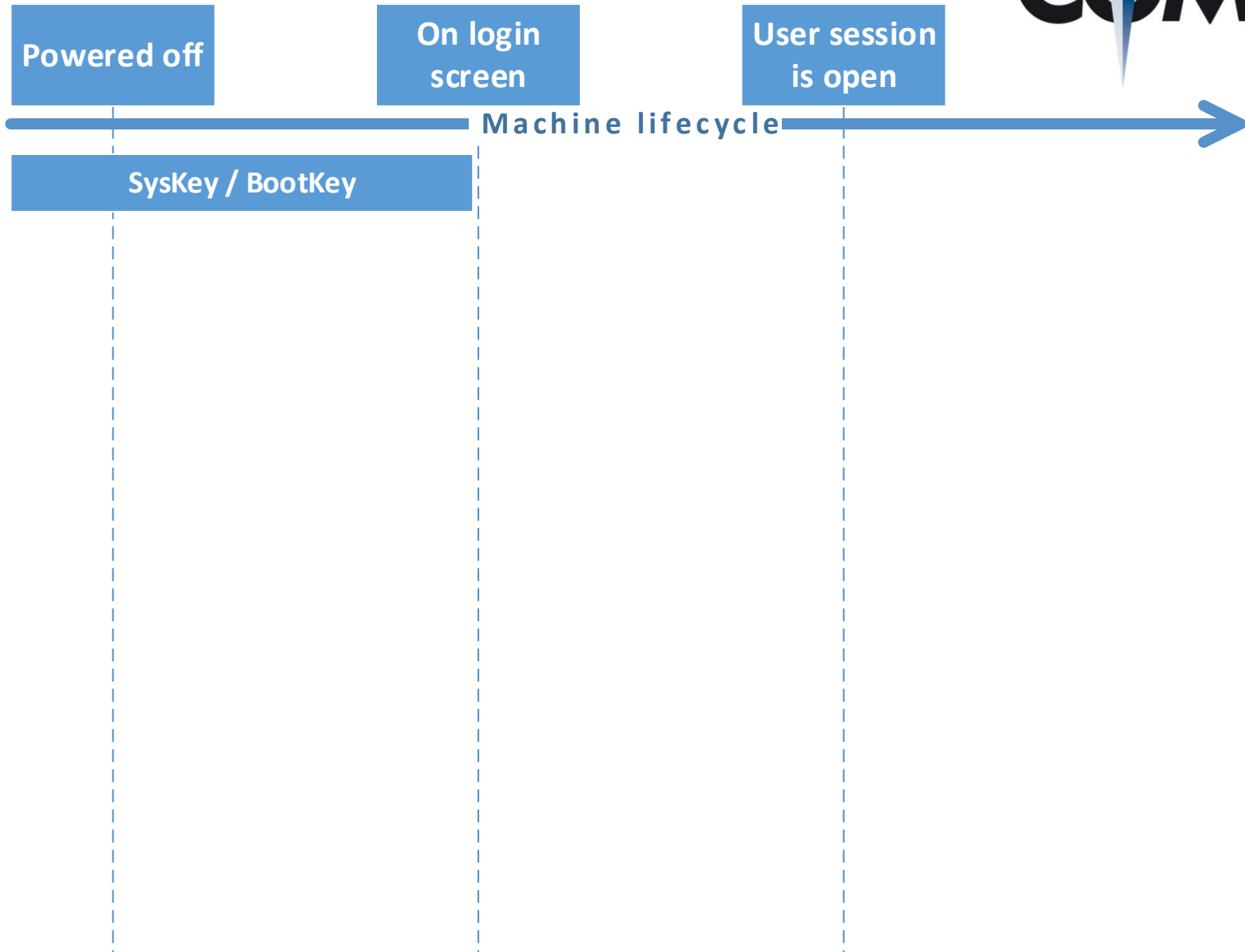
Encrypting File System (EFS)

- ✦ NTFS feature allowing file/folder encryption based on public key system
- ✦ Relies on the Windows Data Protection API (DPAPI) for the keys protection
- ✦ Not implemented in the upcoming new Resilient File System (ReFS)

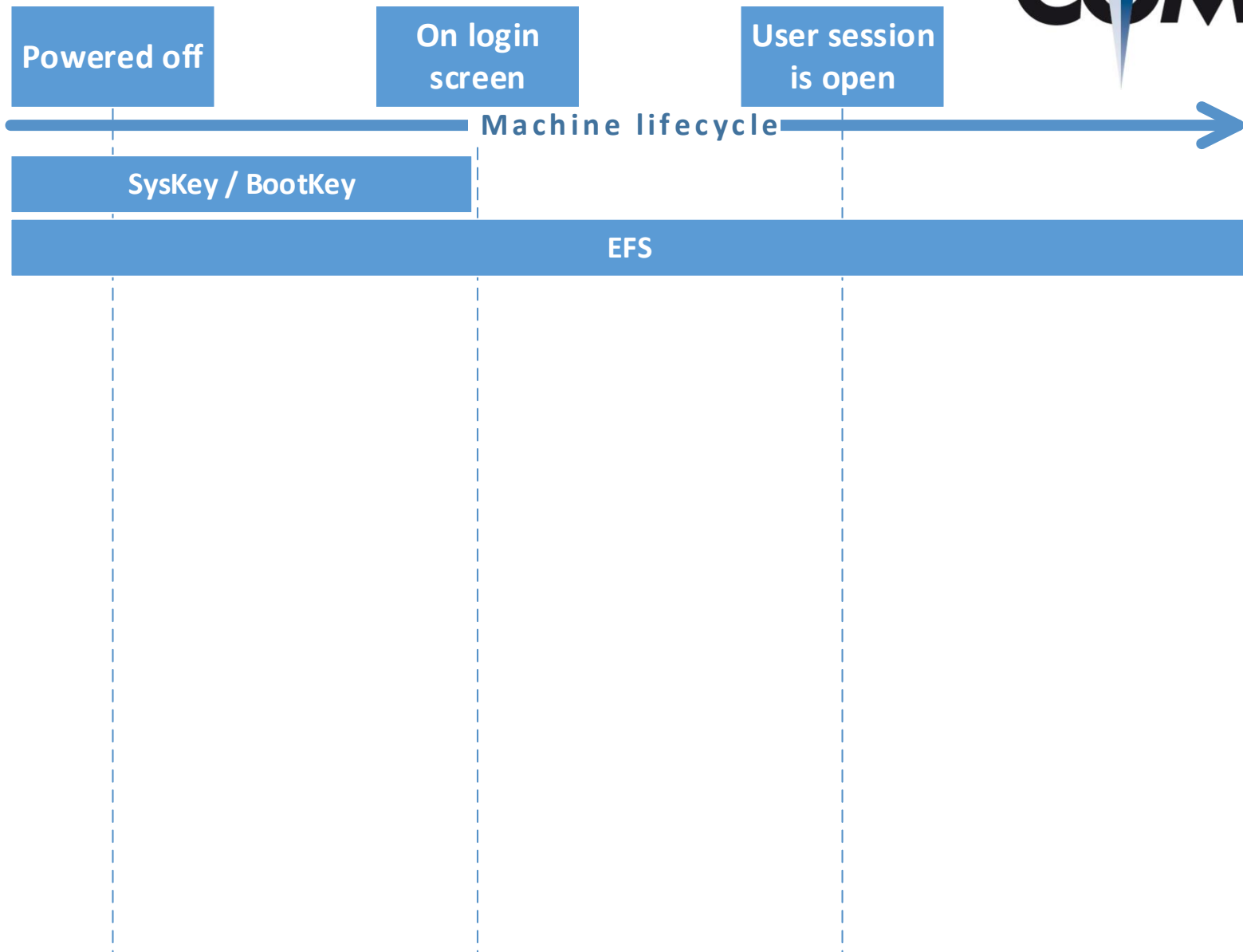
BitLocker

- ✦ Volume based encryption mechanism available since Vista
- ✦ Several research available and getting more and more standard
- ✦ Shifts the focus to the security of the boot process, the PIN+TPM and the AD

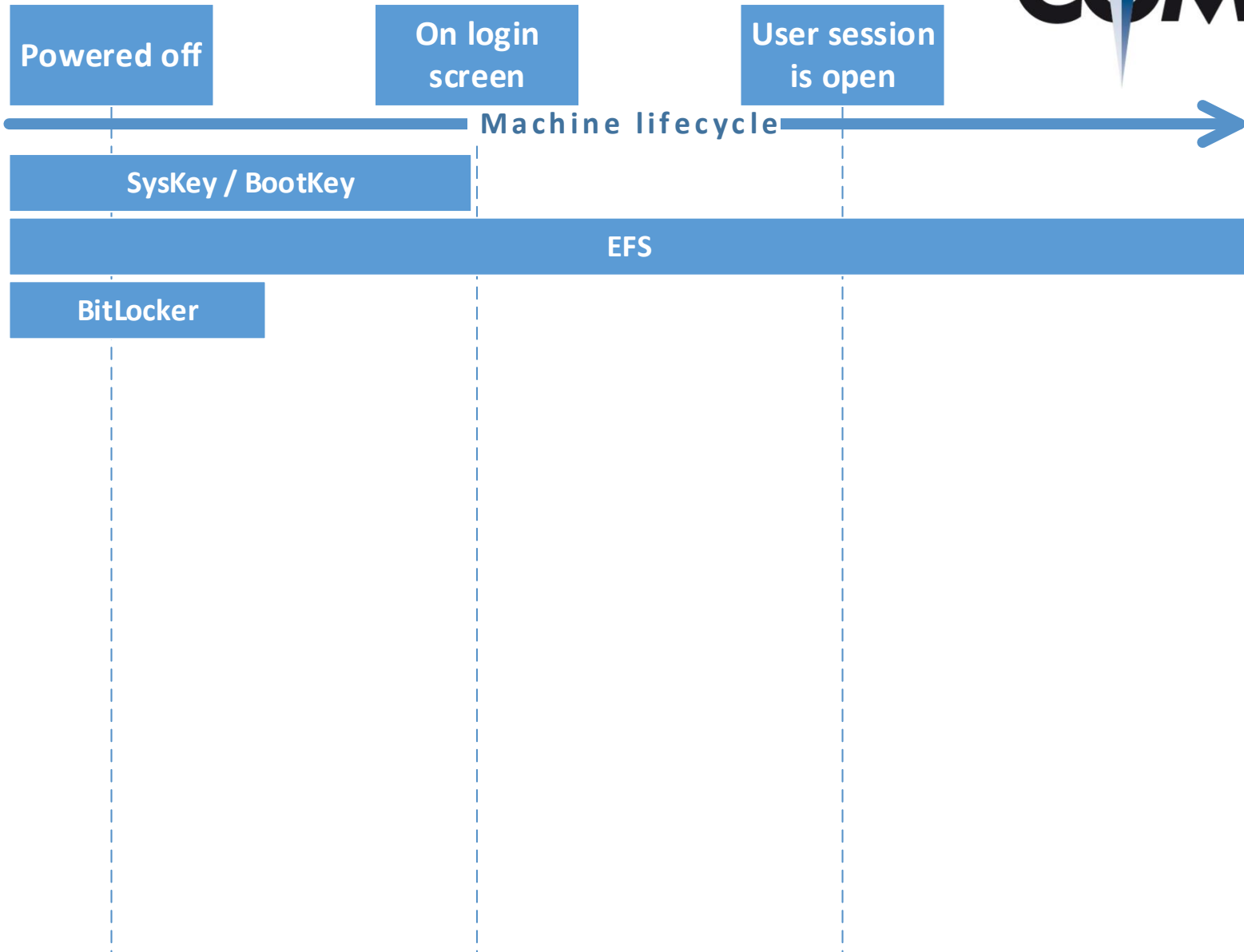
Phase 1 - Security mechanism overview



Phase 1 - Security mechanism overview



Phase 1 - Security mechanism overview



Windows Data Protection API (DPAPI)

- ✦ Central but little known Windows component responsible for storing “secrets”
- ✦ Is used by several other mechanisms (EFS, CryptoAPI, .NET framework, application passwords etc.)
- ✦ Symmetric encryption scheme per user or machine
- ✦ Keeps by design a history of the user’s passwords

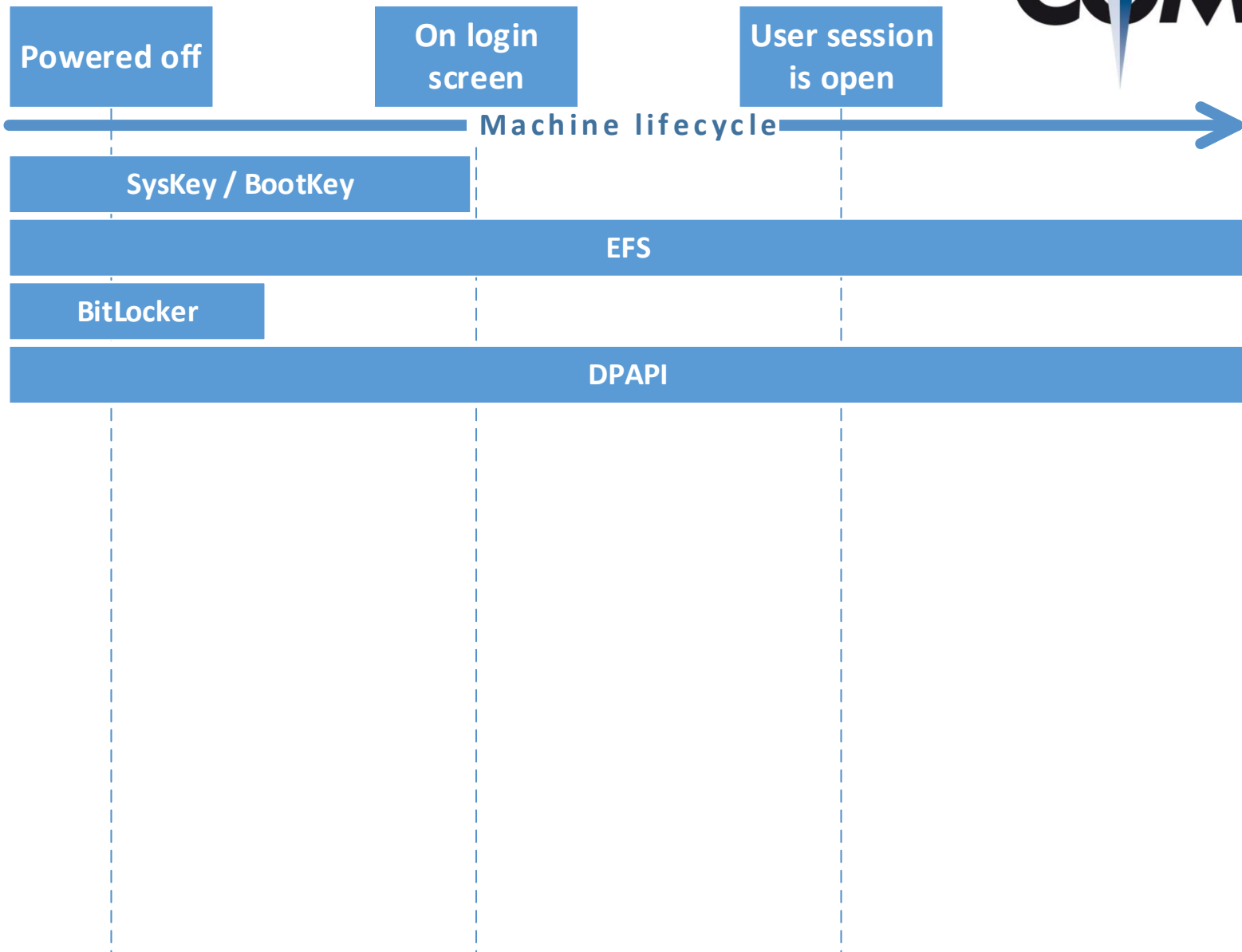
LSASS's LsaProtectMemory method

- ✦ Another core Windows security component recently in the news
- ✦ Several attacks possible by design with local administrator privileges
- ✦ Attack surface reduced with Windows 8.1 – but new features of Mimikatz too!

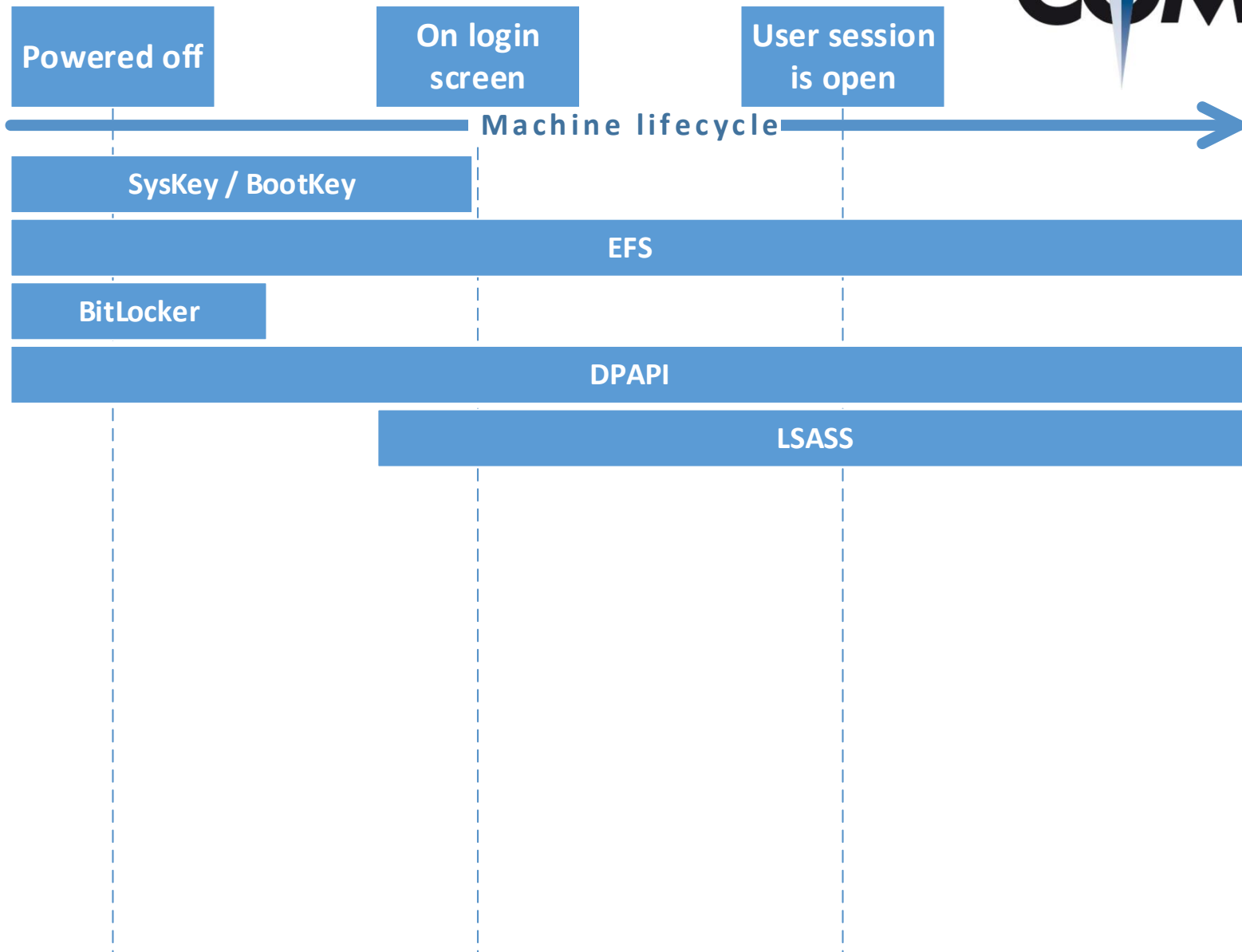
.NET ProtectedMemory, ProtectedData and related methods

- ✦ Methods to protect data in memory, respectively at rest
- ✦ Relies on DPAPI or the machine key mechanism

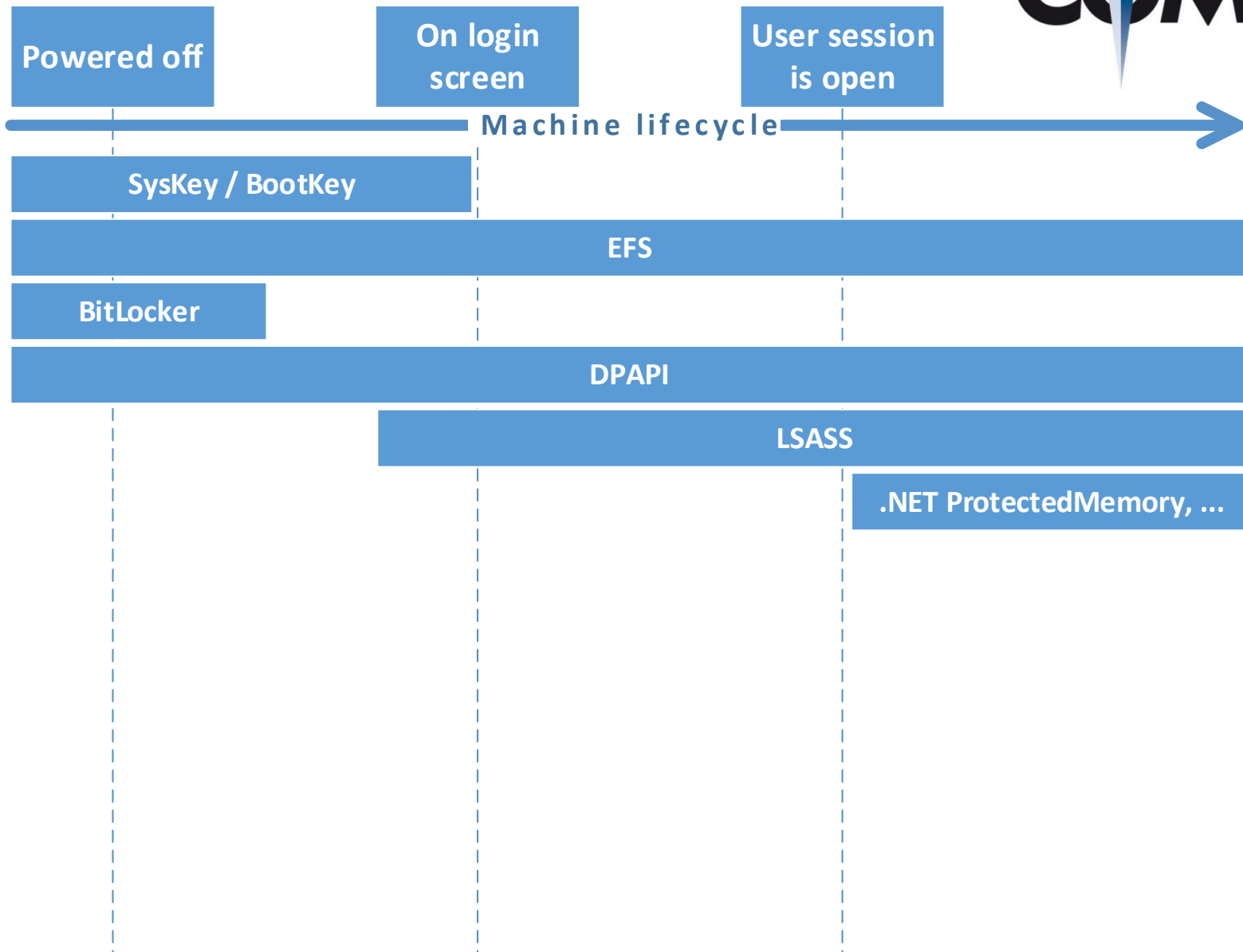
Phase 1 - Security mechanism overview



Phase 1 - Security mechanism overview



Phase 1 - Security mechanism overview



Machine Key mechanism (.NET framework)

- ✦ Set of two keys/algorithm to ensure integrity or perform symmetric encryption
- ✦ Disregarded by developers but essential feature of ASP.NET (ViewState MAC, resource, authentication cookies, membership passwords)
- ✦ Relying on DPAPI – also when the auto-generation of keys is enabled

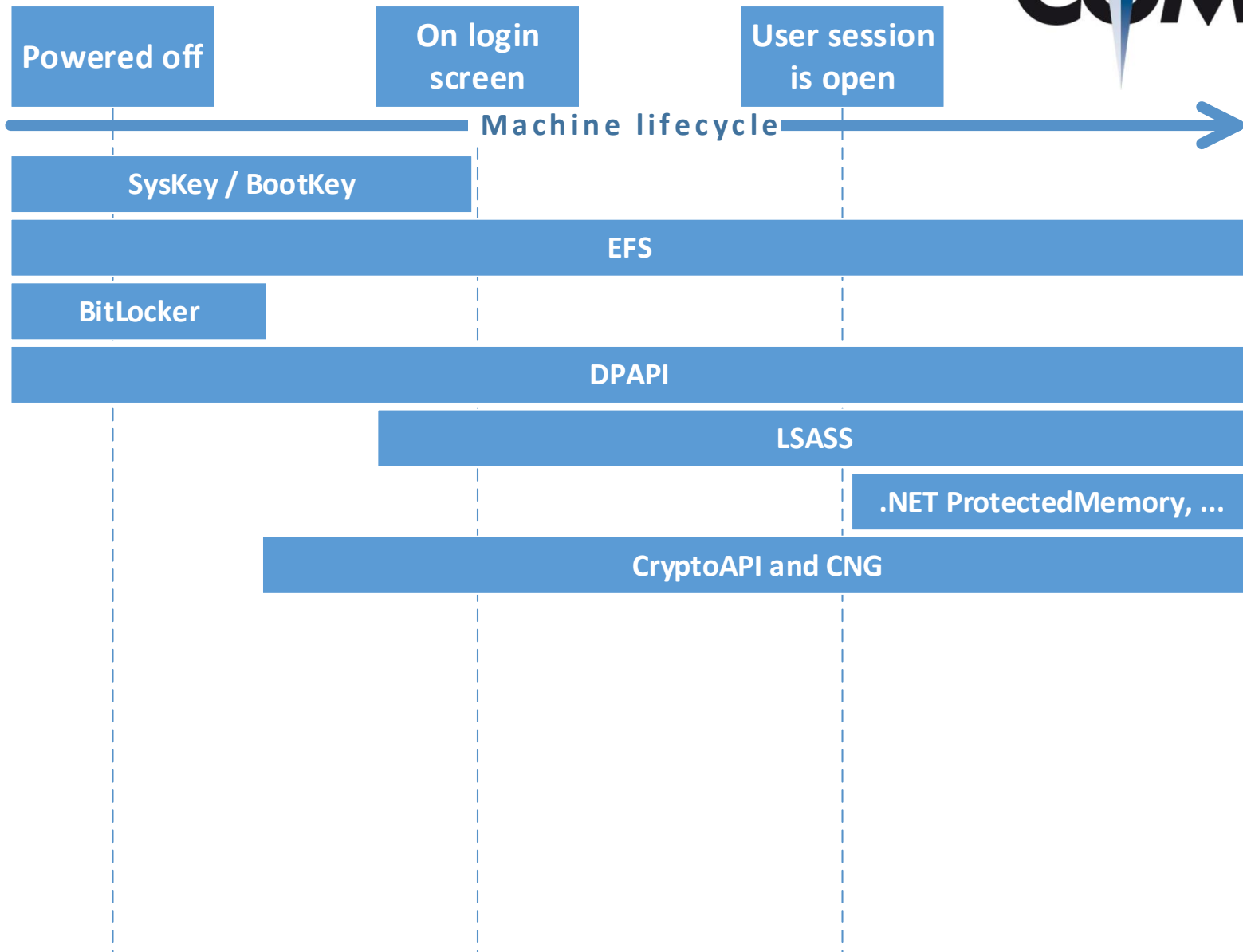
CryptoAPI and Crypto Next Generation (CNG) API

- ✦ Provides a unique interface for crypto operations and manages/stores keys
- ✦ CryptoAPI got replaced by Cryptography API Next Generation (CNG) in Vista
- ✦ Key protection relies on LSASS, unless password-protected or TPM-stored

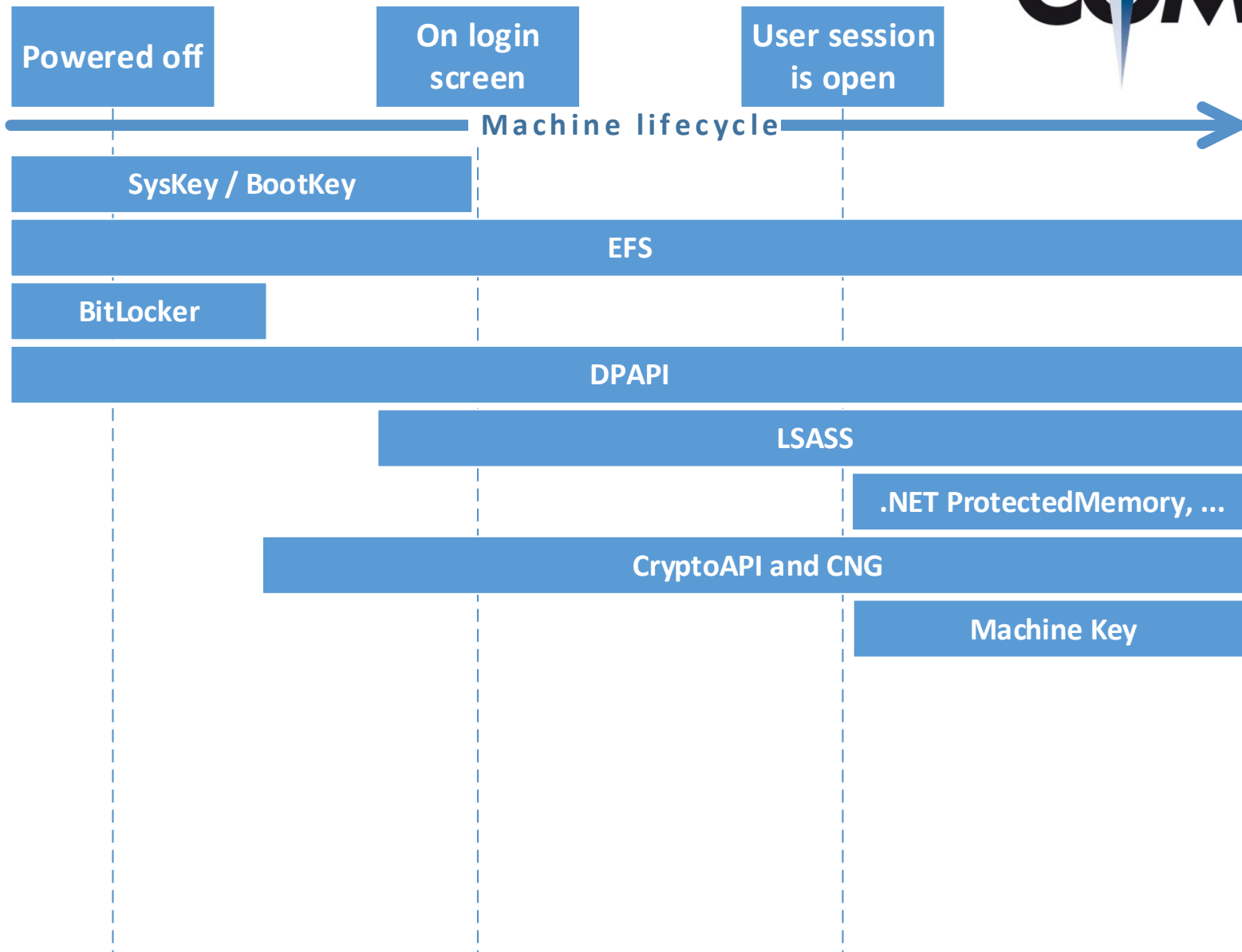
Server Message Block (SMB)

- ✦ Native Windows mechanism to access files over a network
- ✦ SMB version 3 (Win 8/2012) allows encryption on a session or a share basis
- ✦ Unfortunately still weak policies in practices, allowing downgrade attacks

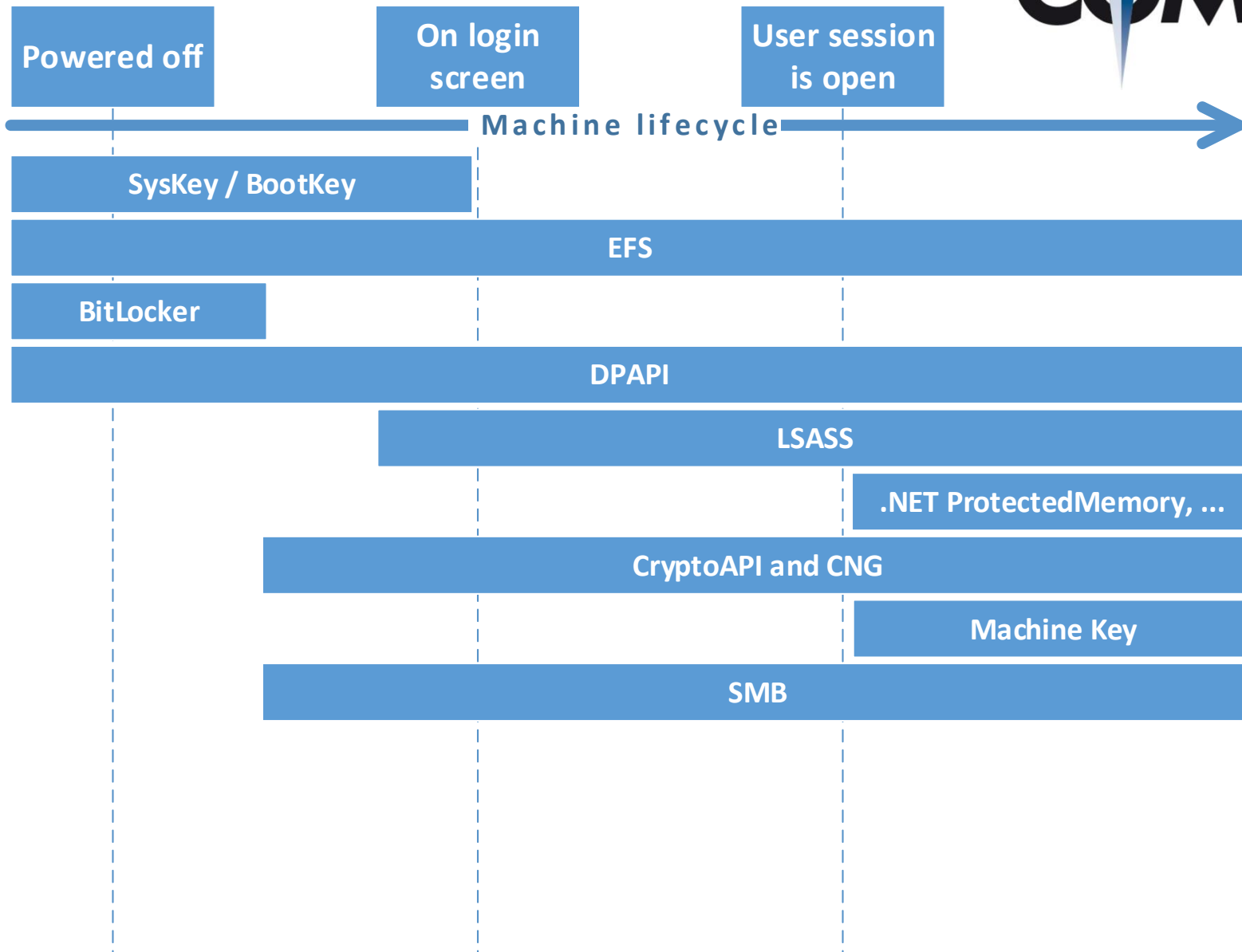
Phase 1 - Security mechanism overview



Phase 1 - Security mechanism overview



Phase 1 - Security mechanism overview



Group Policy Preferences

- ★ New Win 2008 feature to manage preferences, not just policies
- ★ Stores AES-256 encrypted passwords in xml files stored on the DC's share
- ★ Key is here: [http://msdn.microsoft.com/en-us/library/cc422924\(PROT.10\).aspx](http://msdn.microsoft.com/en-us/library/cc422924(PROT.10).aspx)

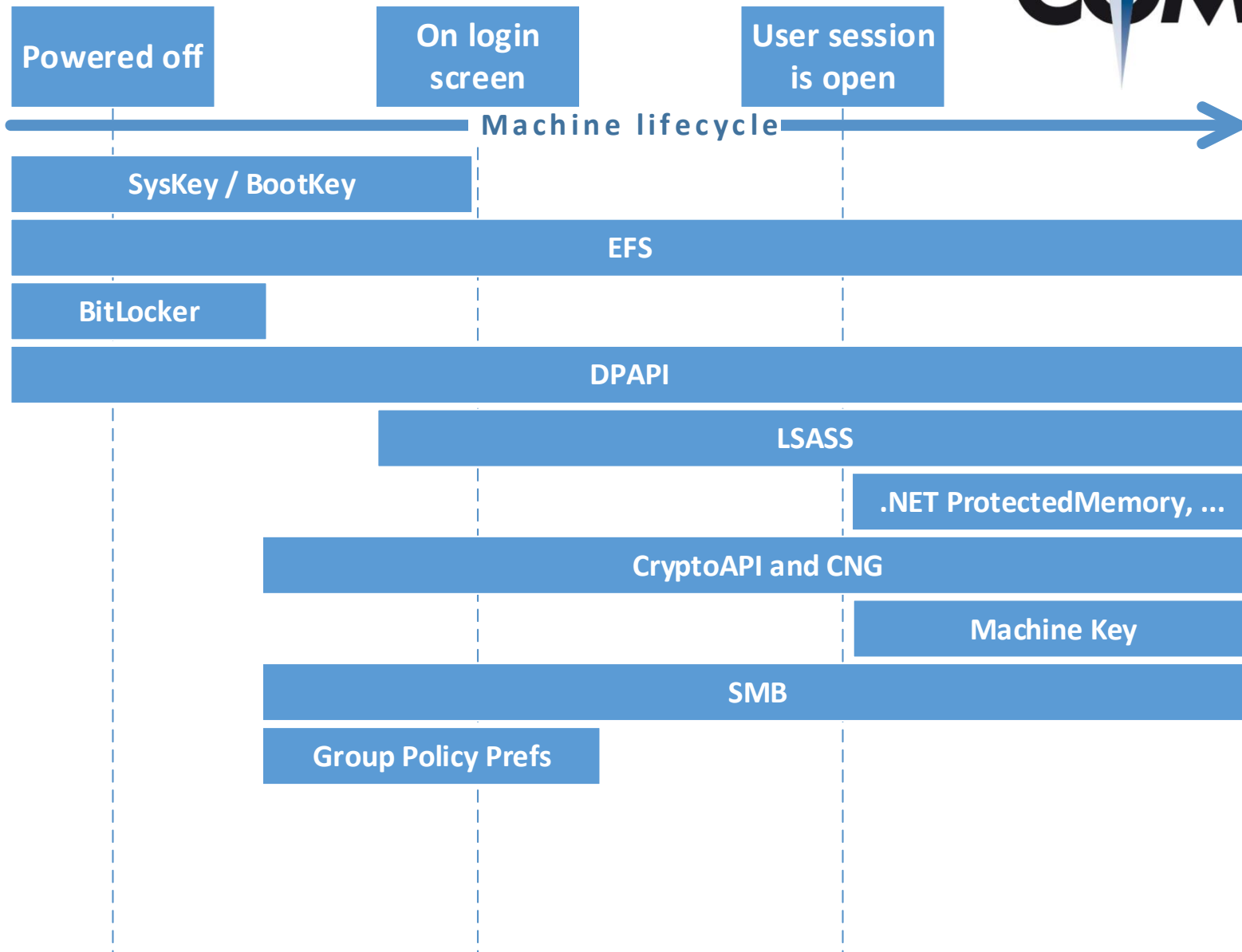
Secure Channel (Schannel)

- ★ Operating system bound SSP for HTTPS communication
- ★ Used e.g. by Internet Explorer as client or IIS as server
- ★ Is the reason why e.g. WinXP (and not IE 6) does not support TLSv1 by default
- ★ Consider tuning accepted ciphers – e.g. via GPOs

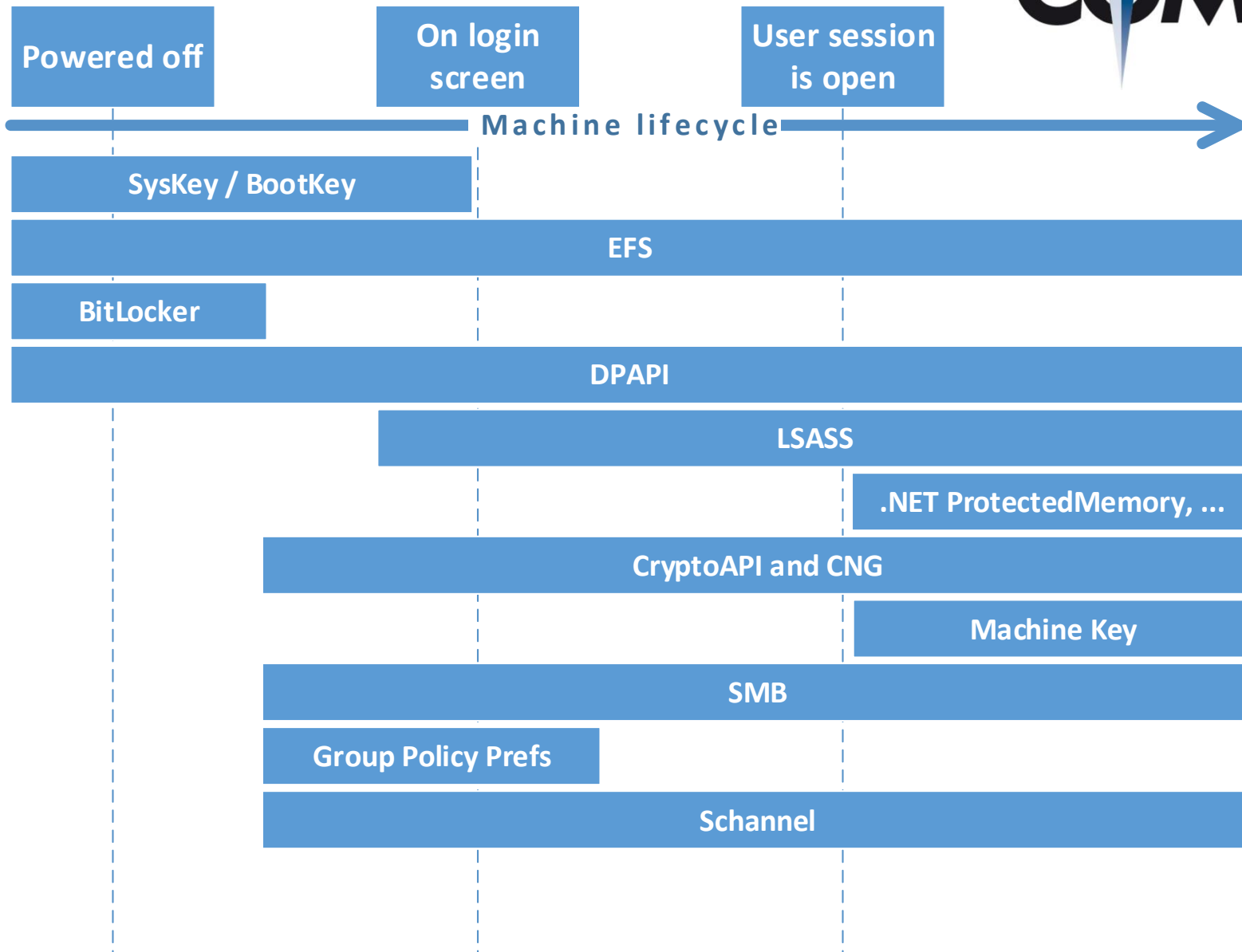
Windows CardSpace

- ★ Claim-based identity model pushed by Microsoft and available in .NET 3.0
- ★ Was relying on DPAPI for the key storage and got discontinued in 2011

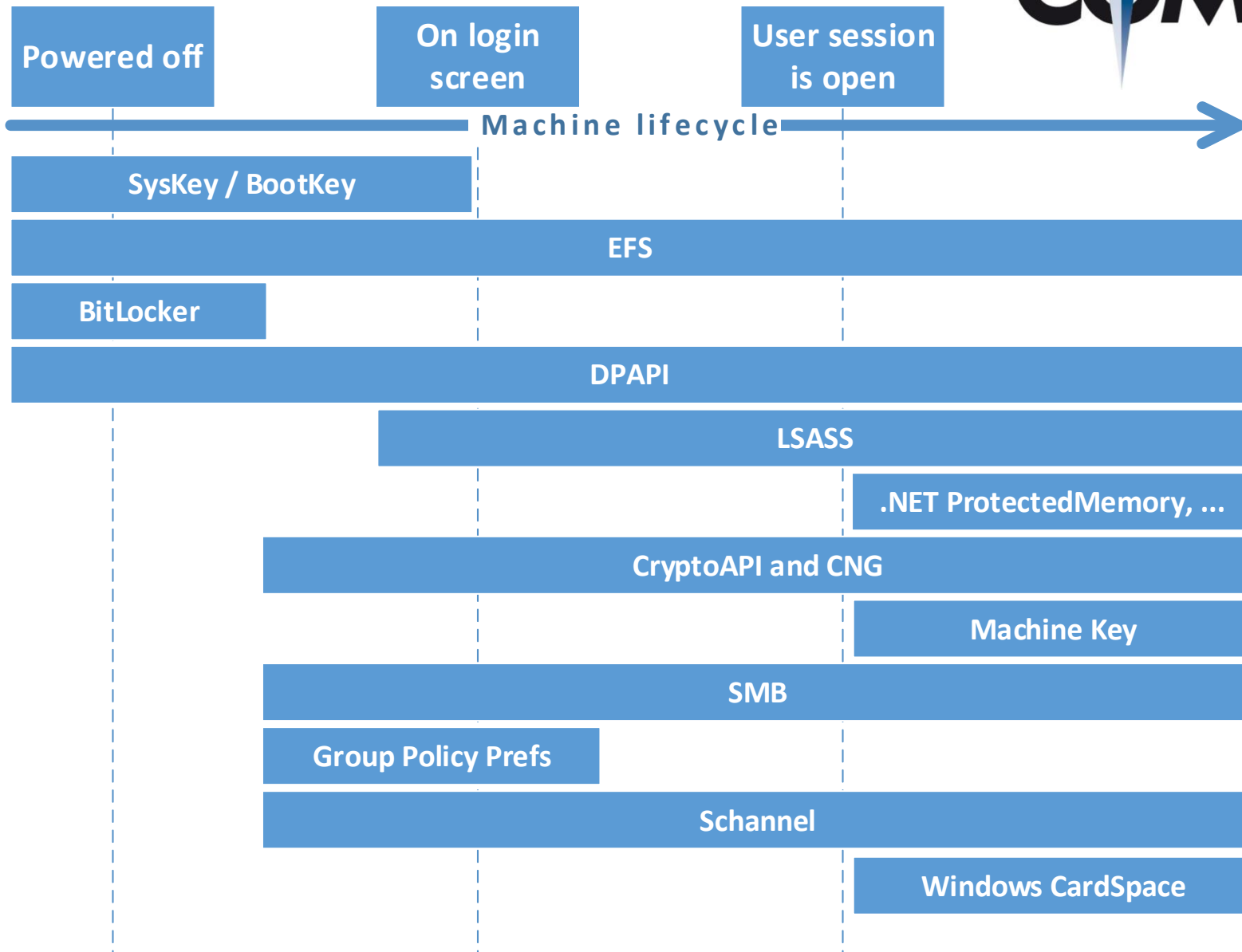
Phase 1 - Security mechanism overview



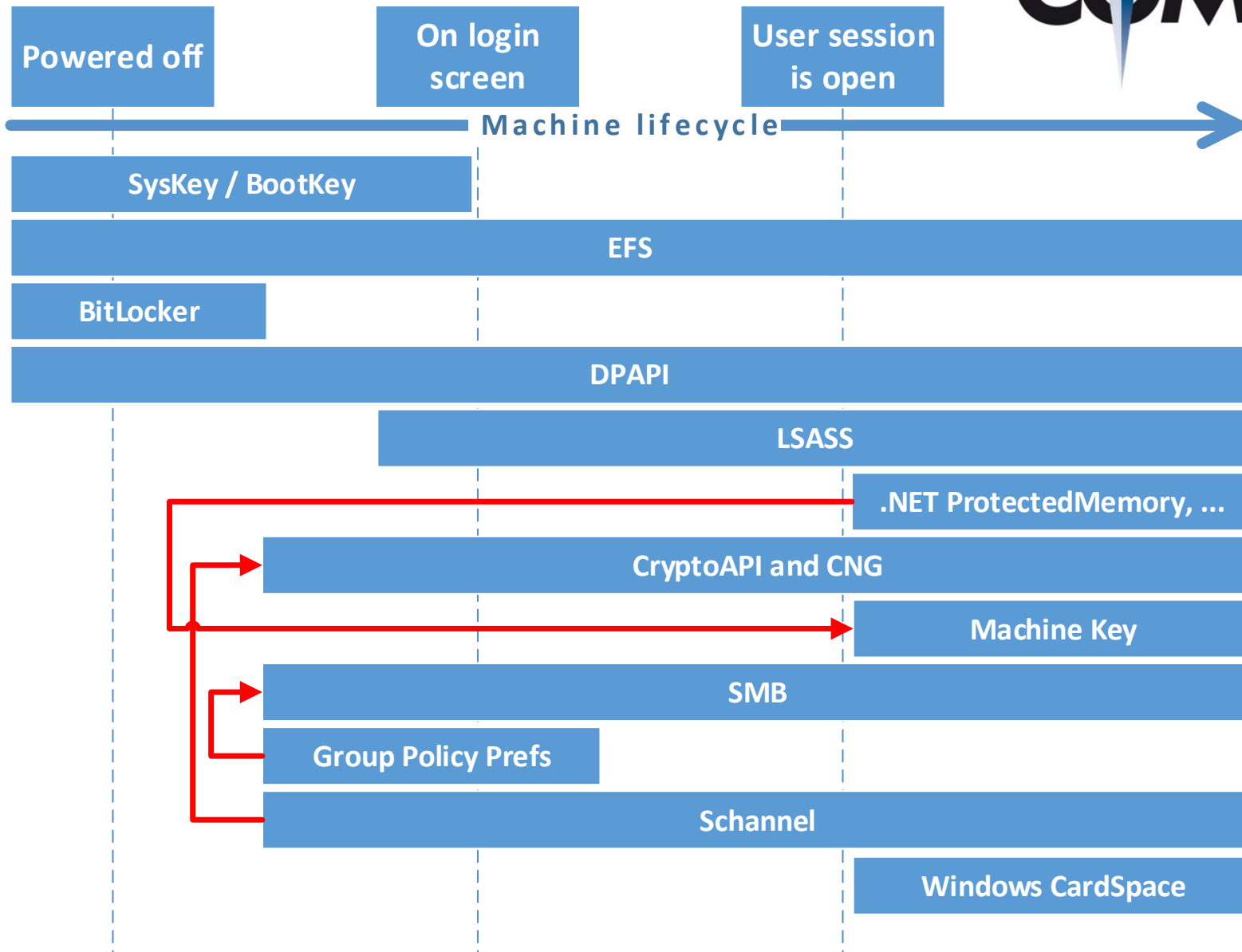
Phase 1 - Security mechanism overview



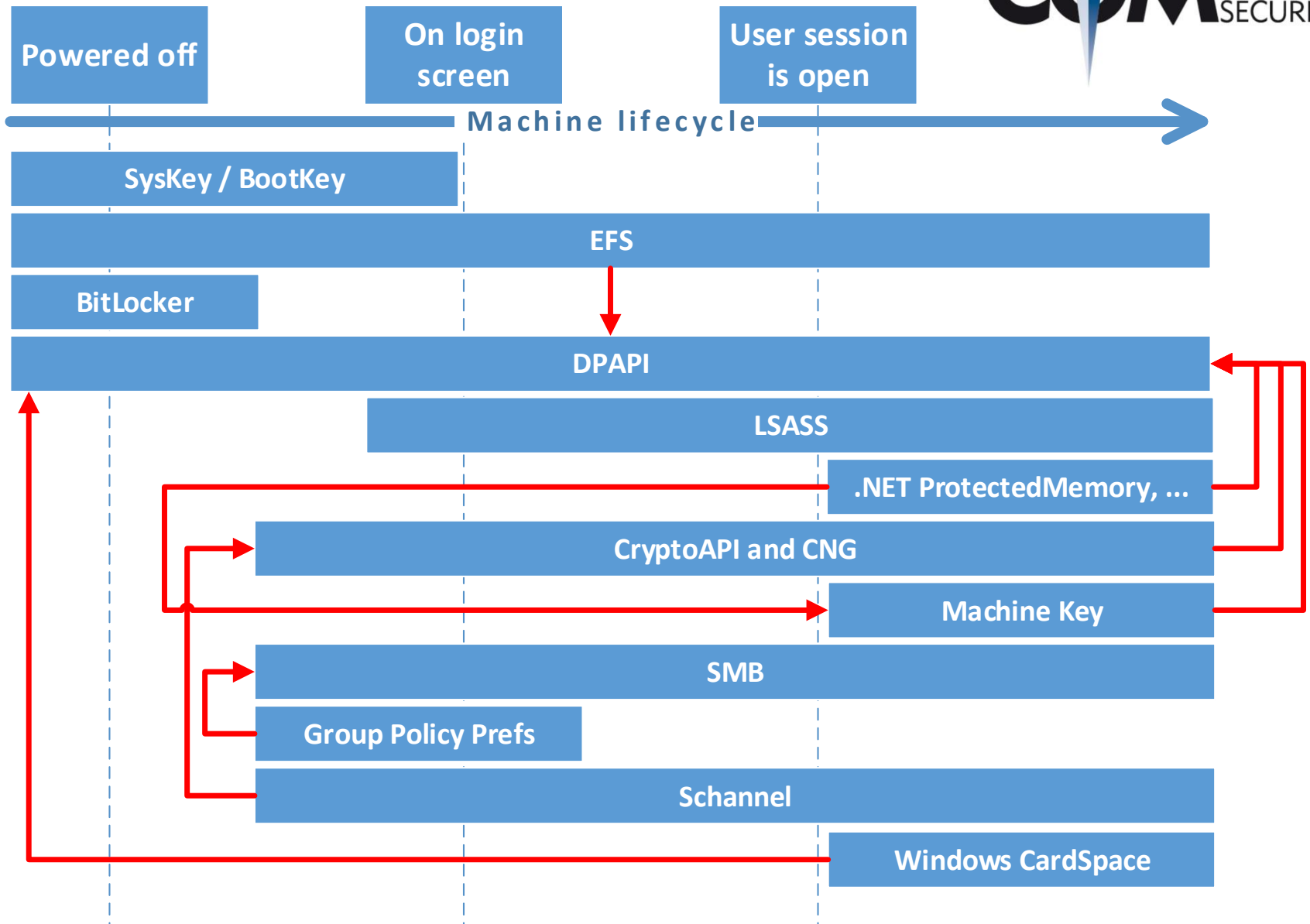
Phase 1 - Security mechanism overview



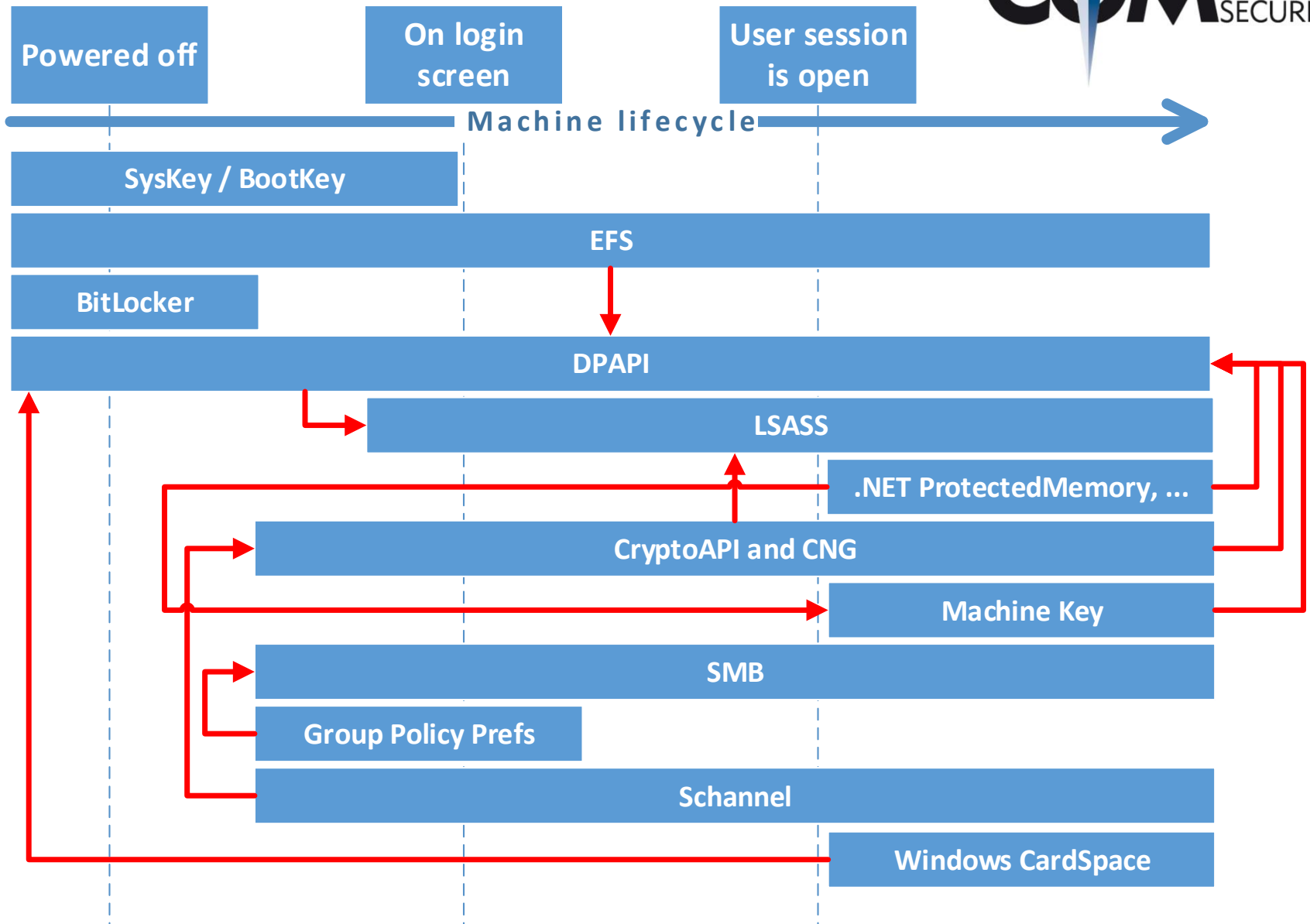
Phase 1 - Security mechanism overview



Phase 1 - Security mechanism overview



Phase 1 - Security mechanism overview



Phase 1 - Security mechanism overview



Rating the importance of the security mechanism based on the following factors:

Adding priority for further studies

- ✦ Importance of protected assets
- ✦ Open questions
- ✦ Importance for the future

Reducing priority for further studies

- ✦ Available research
- ✦ Available tools
- ✦ Support for recent versions

| Description | | Adding factors | | | | Diminishing factors | | | | Priorities | |
|-------------------------------------|------|------------------|----------------|-----------------------|-------|---------------------|-------|------------------------------|-------|--------------------|------|
| Name | Type | Protected assets | Open questions | Importance for future | Total | Research | Tools | Support for recent versions? | Total | Resulting priority | Rank |
| Windows Data Protection API (DPAPI) | OS | 5 | 4 | 4 | 80 | 3 | 3 | 3 | 27 | ↑ 53 | 1 |

Top 3 security mechanisms are:

- ✦ Windows Data Protection API (DPAPI)
- ✦ MachineKey mechanism
- ✦ BitLocker and its new Network Unlock feature

Agenda



Introduction

Work content and methodology

Phase 1 - Security mechanism overview

Phase 2 - In-depth analysis and findings

Recommendations & What's new since its release?

Conclusion

Questions

In scope are for this in-depth analysis are:

- ✦ Windows Data Protection API (DPAPI) (Windows and .NET API)
- ✦ MachineKey mechanism (.NET)
- ✦ BitLocker and its new Network Unlock feature (Windows)

Windows Data Protection API (DPAPI)

- ✦ Performing a password history recovery attack with two different versions of tool dpapick

MachineKey mechanism

- ✦ Audit and exploitation of leaked cryptographic key material
- ✦ Demo

BitLocker and its new Network Unlock feature

- ✦ Theoretical analysis of this new Windows 8 / Windows Server 2012 feature

Windows Data Protection API (DPAPI)


- ✦ Is a central component of the Windows security
- ✦ Is little studied up to now
- ✦ Has only one tool which can read its structures in a generic way (dpapick)
- ✦ Keeps a list of all user's previous passwords called CREDHIST (SHA1(unicode(password)) for Windows XP & Vista)

Performed steps

- ✦ Got familiar with two radically different versions of the same tool (reading source code, drawing class diagram, debugging code, fixing bug, ...)
- ✦ Created a custom script to extract the hashes and successfully ran the attack
- ✦ Experimented various ways to crack the hashes

Conclusion

- ✦ A Trojan can not only access the current password of a user but also its password history
- ✦ The attack is not trivial and only works on Windows XP & Vista (for now)

Recent activity 

Jean-Michel Picod pushed 1 commit to [jmichel/dpapick](#)

17 hours ago

[526659](#) - [fix] missing argument - Thanks Alexandre Herzog

MachineKey mechanism

- ✦ Is where cryptographic key material is managed in (ASP).NET applications
- ✦ Several features of the .NET framework leverage this key material (ViewState, URL and cookie encryption, ...)
- ✦ Was in the headlines in 2010 due to the Padding Oracle attack against .NET
- ✦ MachineKey must be managed if you have load balanced web servers

Performed steps

- ✦ Created an audit tool to automatically survey open source web applications
- ✦ Identified 3 vulnerable web applications and reported them to Microsoft
- ✦ Created a tool (mkleakor) to audit and exploit vulnerable applications

RE: Static machinekey entries [MSRC 15391st]

Conclusion

Microsoft Security Response Center <secure@microsoft.com>

- ✦ You replied to this message on 23.08.2013 07:23. Please do not disclose this information.
- ✦ Proper key management is essential

Sent: Do 22.08.2013 23:21

To: Alexandre Herzog

Cc: Microsoft Security Response Center

Thank you very much for your report. I have opened case 15391 and the case manager, Stephen, will be in touch when there is more information. In the meantime, we ask you respect our coordinated vulnerability disclosure guidelines and not report this publicly until users have an opportunity to protect themselves. You can review our bulletin acknowledgment policy at <http://www.microsoft.com/technet/security/bulletin/policy.mspx> and our

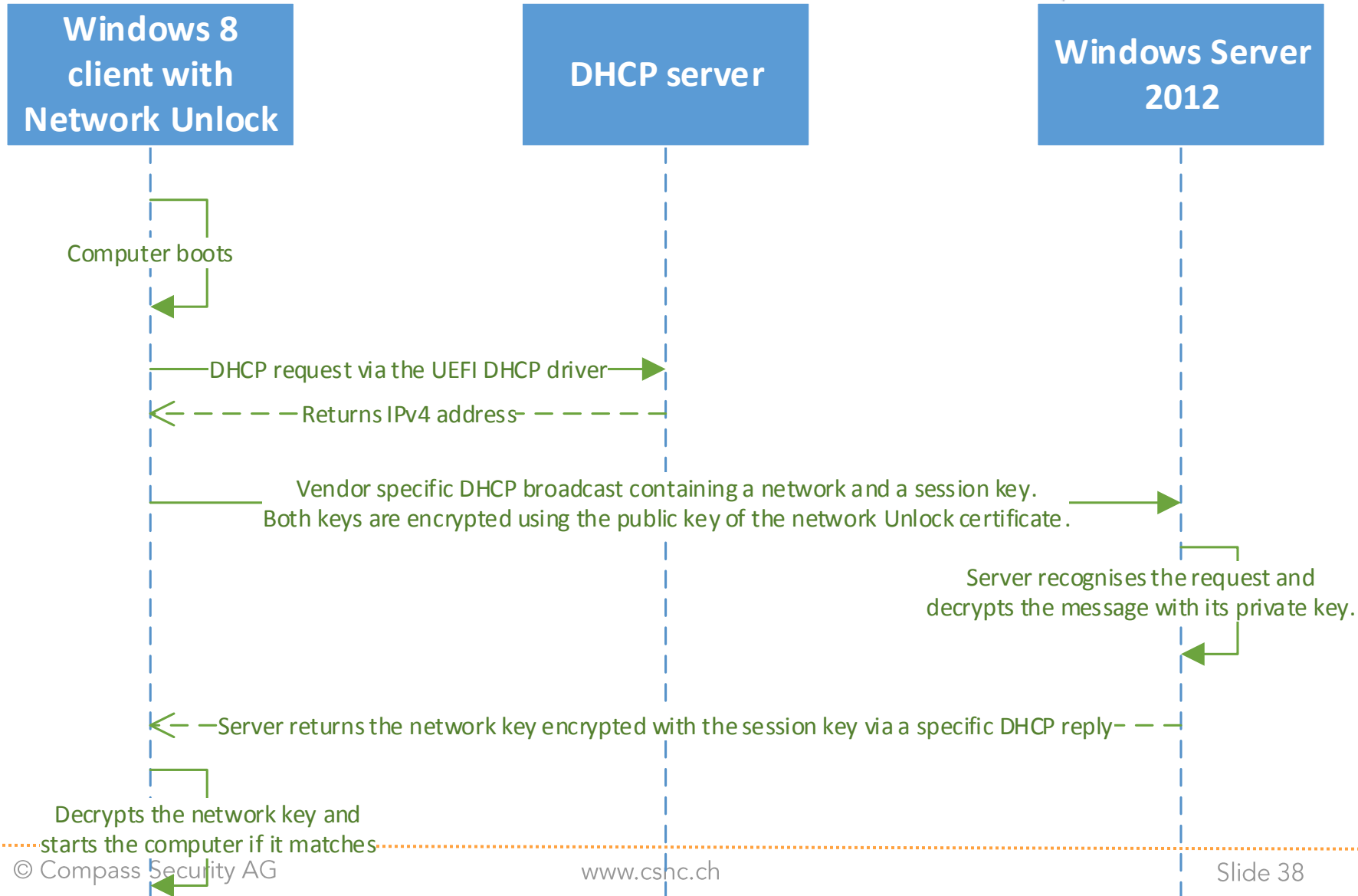
BitLocker and its new Network Unlock feature

- ✦ Is a new feature of Windows 8 and Windows Server 2012
- ✦ Bypasses the entry of a PIN (+TPM) to unlock your hard drive protected by BitLocker, as long as you're connected to the network of your company
- ✦ Is not well documented and had not been studied by the security community

Performed steps

- ✦ Summary of the available documentation, including the different keys and message exchanges (sequence diagram)
- ✦ Identified 6 possible attacks based on the previous review
- ✦ Setup lab to confirm or debunk these attacks, which was not possible to special unmet hardware requirements

Phase 2 - In-depth analysis and findings



BitLocker and its new Network Unlock feature

- ✦ Is a new feature of Windows 8 and Windows Server 2012
- ✦ Bypasses the entry of a PIN (+TPM) to unlock your hard drive protected by BitLocker, as long as you're connected to the network of your company
- ✦ Is not well documented and had not been studied by the security community

Performed steps

- ✦ Summary of the available documentation, including the different keys and message exchanges (sequence diagram)
- ✦ Identified 6 possible attacks based on the previous review
- ✦ Setup lab to confirm or debunk these attacks, which was not possible to special unmet hardware requirements

Conclusion

- ✦ Theoretical study of the new BitLocker Network Unlock
- ✦ Many questions remaining pending about this feature

Agenda



Introduction

Work content and methodology

Phase 1 - Security mechanism overview

Phase 2 - In-depth analysis and findings

Recommendations & What's new since its release?

Conclusion

Questions

What's new since its release?



Machine key issues got fixed

- ✦ Although without any thanks or acknowledgement by any involved party
- ✦ Microsoft plans to release a tool to ease their distribution and management

Microsoft is working on the Group policy preference issues

- ✦ *"We planed to disable the feature but customers wanted to keep it despite the involved risks"*

Microsoft is improving some security aspects of Windows...

... but Mimikatz continued to up with new attack scenarios too

- ✦ Extract credentials based on a process dump of LSASS
- ✦ Golden Kerberos tickets & extracting the Smart Card PIN
- ✦ Started playing with DPAPI related structures...

Still many other points to dig in and research!

- ✦ The MAS thesis will be published on <http://blog.csnc.ch> soon

Consider reading the full paper once published, but in a nutshell:

- ✦ Use a Whole Disk Encryption solution with UEFI's Secure Boot and a strong second factor (at least PIN+TPM)
- ✦ Ensure your TPM are secure and use them (e.g. for BitLocker or certificates)
- ✦ Reduce administrator privileges as much as possible across the domain
- ✦ While handling incidents, assume the attacker not only compromised the current password but also all its history
- ✦ Ensure your applications rely as often as possible on Windows logins but consider disabling delegation for sensitive accounts
- ✦ Recognise the machine keys being cryptographic material and manage them accordingly
- ✦ Harden the Windows settings (e.g. via GPOs), e.g. in regards of SChannel, SMB communication; ensure you don't manage passwords within GPPs

You can achieve a lot with a good Windows hardening

- ✦ But beware as attackers will shift their focus towards other targets (e.g. Domain Controllers, BIOS, physical attacks etc.)

Agenda



Introduction

Work content and methodology

Phase 1 - Security mechanism overview

Phase 2 - In-depth analysis and findings

Recommendations & What's new since its release?

Conclusion

Questions

Phase 1 - Security mechanism overview featured

- ✦ A comprehensive list of all crypto-based security mechanisms in Windows and in the .NET framework
- ✦ Details about each security mechanisms and its dependencies
- ✦ Possible attacks and state-of-the-art countermeasures and recommendations

Phase 2 - In-depth analysis and findings

- ✦ Enlightened 3 selected security mechanisms
- ✦ Identified new attack vectors and vulnerable applications
- ✦ Contributed patches or tools for further audit and exploitation

This work

- ✦ Aims to be a reference for best practices, further documentation and a starting point for additional research
- ✦ Was, on a personal note, a challenging and demanding task, requiring many different kinds of skills and dedication all over its realisation
- ✦ **Was, on a personal note, not only interesting to realise but also fun!**

Thank you for your attention

alexandre.herzog@csnc.ch

<http://blog.csnc.ch/author/aherzog/>

<http://ch.linkedin.com/in/alexandreherzog>