

# RSA<sup>®</sup>Conference2019

San Francisco | March 4–8 | Moscone Center



**BETTER.**

SESSION ID: KEY-T06S

## Top 10 ways to make hackers excited: All about the shortcuts not worth taking



**Paula Januszkiewicz**

CQURE: CEO, Penetration Tester / Security Expert

CQURE Academy: Trainer

MVP: Enterprise Security, MCT

Microsoft Regional Director

Contact: [paula@cquire.us](mailto:paula@cquire.us) | <http://cquire.us>



@paulacquire  
@CQUREAcademy

#RSAC



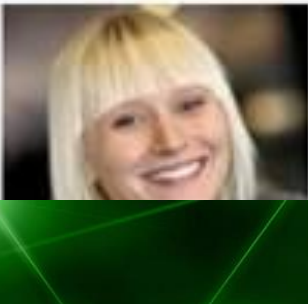
Featured TechEd 2012 Speakers [More featured speakers →](#)



Wally Mead



John Craddock



We are proud to announce that **Paula Januszkiewicz** was rated as **No 1 Speaker** at Microsoft Ignite!!!

May 4-8, 2015  
Chicago, IL

[ATTEND](#) [TRAININGS](#) [BRIEFINGS](#) [ARSENAL](#) [FEATURES](#) [SCHEDULE](#) [SPECIAL EVENTS](#)

[SEE ALL PRESENTERS](#) **SPEAKER**

**PAULA JANUSZKIEWICZ**  
CQURE INC.

Paula Januszkiewicz is a CEO and Founder of CQURE, a security consulting firm. She is also an Enterprise Security MVP and a well-known speaker at security conferences. Customers all around the world. She has a deep belief that positive thinking is key to success and pays extreme attention to details and conference content.

CONFERENCE

安全国际论坛  
INFOSEC Forum  
CHINA 2011

Where The World Talks Security  
November 2 – 3  
China World Hotel  
Beijing, China

Learn. Connect. Collaborate.

Join us in Madrid

the adventures of **alice & bob**

Registration & Accommodation

Agenda & Sessions

Sponsors

Contact Us

Brad Anderson

Jon DeVaan

Mark Russinovich

Brian Keller

Paula Januszkiewicz

Mark Minasi

Jeffrey Snover

John Craddock

Scott Woodgate

Marcus Murray

Wednesday, November 2

Thursday, November 3

General Sessions

Applications and Development

Cryptography and Architecture

Hackers and Threats

Mobile and Network Security

Trusted and Cloud Computing

**Mark Kennedy**  
Symantec  
Topic: Anti-Malware Industry... Cooperating. Are You Serious?

**Samir Saklikar**  
Dennis Moreau  
RSA, The Security Division of EMC

**Marc Bown**  
Trustwave  
Topic: APAC Data Compromise Trends

**Paula Januszkiewicz**  
CQURE  
Topic: Password Secrets Revealed! All You Want to Know





Technical systems are:  
**Reviewed**  
**Scanned**  
**Penetration Tested**

So?





# 1<sup>st</sup> Way: Disabling firewall / misconfigured network access

## Key learning points:

- ✓ Windows Firewall is often misconfigured
- ✓ Firewall is a great segmentation tool
- ✓ You can allow only certain processes to communicate with the Internet or locally
- ✓ No need to know processes to block them, you can operate on the services list

In Windows Firewall there are couple of things missing:

- x Filtering by the group of computers
- x Detailed logging for network traffic
- x Expandability – there are not many options
- x No correlation in between process and network traffic – whose role is this?



# Demo: File download + DNS Exfiltration



## 2<sup>nd</sup> Way: Overly simple passwords and security questions

### Key learning points:

- ✓ Almost always there are passwords reused
- ✓ Almost always (ekhm... always) there is some variant of company name and some number (year, month etc.)
- ✓ It makes sense to check for obvious passwords and continuously deliver security awareness campaigns

### Typical password locations

NTDS.dit, SAM

Configuration files

Registry

Memory dumps, Hiberfil.sys

Databases (DPAPI ?)



# Demo: Simple checks needed



## 3<sup>rd</sup> Way: No network segmentation

### Key learning points:

- ✓ Network segmentation can be a blessing or a curse
- ✓ Greater control over who has access to what
- ✓ Allows to set rules to limit traffic between each distinct subnet
- ✓ Allows to reduce exposure to security incidents
- ✓ Performance: allows to reduce Broadcast Domains so that broadcasts do not spread on the entire network
- x VLANs limit – only 4094 different VLANs for the same network
- x Security limits – geo locations vs. ATM clouds
- x Managerial overhead

No-brainer or unseen network security threat?



# Demo: ARP Spoofing on Windows



## 4<sup>th</sup> Way: Lack of SMB Signing (or alternative)

### Key learning points:

- ✓ Set SPNs for services to avoid NTLM:  
*SetSPN -L <your service account for AGPM/SQL/Exch/Custom>*  
*SetSPN -A Servicename/FQDN of hostname/FQDN of domain domain\serviceaccount*
- ✓ Reconsider using Kerberos authentication all over  
<https://technet.microsoft.com/en-us/library/jj865668.aspx>
- ✓ Require SPN target name validation  
*Microsoft network server: Server SPN target name validation level*
- ✓ Reconsider turning on SMB Signing
- ✓ Reconsider port filtering
- ✓ Reconsider code execution prevention but do not forget that this attack leverages administrative accounts



# Demo: SMB Relay



# 5<sup>th</sup> Way: Allowing unusual code execution

## Key learning points:

Common file formats containing malware are:

- ✓ **.exe** (Executables, GUI, CUI, and all variants like SCR, CPL etc)
- ✓ **.dll** (Dynamic Link Libraries)
- ✓ **.vbs** (Script files like JS, JSE, VBS, VBE, PS1, PS2, CHM, BAT, COM, CMD etc)
- ✓ **.docm, .xlsm** etc. (Office Macro files)
- ✓ **.other** (*LNK, PDF, PIF, etc.*)

If **SafeDllSearchMode** is enabled, the search order is as follows:

1. The directory from which the application loaded
2. The system directory
3. The 16-bit system directory
4. The Windows directory
5. **The current directory**
6. The directories that are listed in the PATH environment variable



# Demo: Sneaky code runs



## 6<sup>th</sup> Way: No whitelisting on board

### Key learning points:

- ✓ Code execution prevention implementation is a must
- ✓ PowerShell is an ultimate hacking tool, possible solutions: block it for users, use Just Enough Administration etc.
- ✓ Verify where users have write access to: `accesschk.exe -w .\users c:\windows`
- ✓ AppLocker can run in the audit mode

x AppLocker is great but not with the default configuration

### Machine learning for threat protection:

- ✓ Modern solutions are capable of machine learning but it takes time
- ✓ Modern solutions are quite easy to implement but require a lot of understanding of what they actually do – your call



# Demo: Shares under pressure



# 7<sup>th</sup> Way: Old protocols or their default settings

## Key learning points:

- ✓ SNMPv3 addresses: user-based system for access control, a means to properly authenticate users, and a method for encrypting SNMP traffic between agent and host
- ✓ SQL issues – TDS provides by default lack of encryption
- ✓ ODBC Driver – check if it has a secure networking layer built into it

## NTLMv1 / NTLMv2

- ✓ Security Options in GPO allow to monitor where NTLM is used
- ✓ General direction is to get rid of NTLM

## SSL / TLS

- ✓ TLS v1.3 is still an Internet Draft
- ✓ SSL 2.0 and 3.0 have been deprecated by the IETF (in 2011 and 2015)
- ✓ Disable SSL 2.0 and 3.0, leaving only TLS protocols enabled



# Demo: Injection for TDS

# 8<sup>th</sup> Way: Trusting solutions without knowing how to break them

## Key learning points:

- ✓ The best operators won't use a component until they know how it breaks.
- ✓ Almost each solution has some 'backdoor weakness'
- ✓ Some antivirus solutions can be stopped by SDDL modification for their services
- ✓ Configuration can be monitored by Desired State Configuration (DSC)
- ✓ DSC if not configured properly will not be able to spot internal service configuration changes

Example: how to I get to the password management portal?





# Demo: Sysmon Under Pressure

# 9<sup>th</sup> Way: Misusing service accounts + privileged accounts

## Key learning points:

- ✓ gMSA can also be used for the attack
- ✓ Service accounts' passwords are in the registry, available online and offline
- ✓ A privileged user is someone who has administrative access to critical systems
- ✓ Privileged users have sometimes more access than we think (see: SeBackupRead privilege or SeDebugPrivilege)
- ✓ Privileged users have possibility to read SYSTEM and SECURITY hives from the registry

Warning! Enabling Credential Guard blocks:

- x Kerberos DES encryption support
- x Kerberos unconstrained delegation
- x Extracting the Kerberos TGT
- x NTLMv1



# Demo: Service Accounts + Passwords



# 10<sup>th</sup> Way: Falling for hipster tools

## Key learning points:

- ✓ Worldwide spending on information security is expected to reach **\$90 billion in 2017**, an increase of **7.6 percent over 2016**, and to top \$113 billion by 2020, according to advisory firm Gartner
- ✓ With increasing budget the risk of possessing hipster tools increases too – do we know where these tools come from and what are their security practices?
- ✓ Lots of solutions where not created according to the good security practices (backup software running as Domain Admin etc.)
- ✓ Each app running in the user's context **has access to secrets** of other apps – Data Protection API
- ✓ Case of CCleaner



# Demo: KeePass Under Pressure

# Summary: 10 ways to make hackers happy

## Short term

Isolate infrastructure components so that in case of attack they prevent spreading

Engage with the network security guys

Review servers' and workstations' configuration periodically

## Medium term

Put on the Hacker's Shoes

External + Internal + Web Penetration tests

Configuration reviews

## Long term

Prevention and Vulnerability Management

Start implementing the monitoring and execution prevention





# **RSA**Conference2019

**Session Summary and Tools:**

**<https://cqu.re/keynotersa>**

# RSA<sup>®</sup>Conference2019

## Thank you!

Paula Januszkiewicz

[paula@cqure.us](mailto:paula@cqure.us)

<http://cqure.us>



@paulacquire

@CQUREAcademy