Date/Time: Fr. 17.01.2014 – 18:30h CET

Location: Restaurant Mehlfeld's
81375 München, Guardinistr. 98 a
MVV: U6 Haderner Stern (13 min vom Marienplatz)

Event: **CryptoParty #CPMUC** – nicht nur für Mobilisten
Workshop Digitale Selbstverteidigung
Schwerpunkte Mobile Security + verschlüsselte Kommunikation
für Android, iOS, Windows Phone, Windows, Mac, Linux

Featuring: Roland Jungnickel (@ValiDOM),
Piratenpartei (Vorsitzender Bezirk Oberbayern), EFF, FoeBud, AK Vorrat, ...
Thomas Pfeiffer (@codeispoetry),
WebEvangelisten.de, Bündnis 90 / Die Grünen
Jimmy Schulz (@jimmyschulz),
F.D.P. (Vorsitzender Bezirk Oberbayern), CyberSolutions Ltd.
Franz Haslbeck (@m_o_n_a_c_o),
Consultant ENTERPRISE MOBILITY, Organisator + Moderator
Cristian Mudure (@stackfieldapp),
Gründer + Geschäftsführer, Stackfield GmbH
Joachim Hummel (@JoachimHummel),
Dipl. Elektrotechnik + IT Senior Consultant, unixweb - internet solutions

Anmeldung: Eventbrite (kostenfrei)
http://cryptoparty-muc-20140117.eventbrite.de

Wichtig: Bring Your Own Device !
Bringt Eure eigenen Smartphones, Tablets, Notebooks mit.
Und: ladet Euch vorher die Tools herunter und installiert sie.

Zielgruppe: ambitionierte Einsteiger, Nerds, IT Pros, ... jeder.
Besondere Vorkenntnisse sind nicht erforderlich.

< QR-Code zur Anmeldung auf Eventbrite ;-)

Hashtags:

#CPMUC #CryptoParty #MobileSecurity @enterprisemobi

Links zu Experten:

http://roland-jungnickel.de/roland-jungnickel-pirat/
http://thomas-pfeiffer.de/kontakt/
http://www.jimmy-schulz.com/content/impressum-datenschutz
http://www.xing.com/profiles/Franz_Haslbeck
http://www.linkedin.com/profile/view?id=10486860
http://blog.unixweb.de/

Für die verschlüsselte Kommunikation mit den Experten / zum Testen im Workshop:

- Name	/ Threema ID	/ eMail-Adresse	/ OpenPGP Public Key

- Roland Jungnickel / B82CTDC5 / vali@validom.de
http://pgp.mit.edu:11371/pks/lookup?op=get&search=0x64C54D373A4B0B6A

- Tom Pfeiffer / --- / webevangelisten@gmail.com
http://pgp.mit.edu:11371/pks/lookup?op=get&search=0xE967FFCC33A528B9

- Jimmy Schulz / NE7NBPMW / schulz@jimmy-schulz.de
http://pgp.mit.edu:11371/pks/lookup?op=get&search=0x799E99E9DA766F9A

- Franz Haslbeck / PXCCWTKB / franz.haslbeck@googlemail.com
http://pgp.mit.edu:11371/pks/lookup?op=get&search=0x5D4397DAAE28285E

- Joachim Hummel / 44EWCYWS / jh@unixweb.de
http://pgp.mit.edu:11371/pks/lookup?op=get&search=0xCEFC0372E472D764

Links der Experten zu Inhalten:

http://thomas-pfeiffer.de/linkliste-mailverschluesselung/
http://www.jimmy-schulz.com/content/so-sch%C3%BCtze-ich-mich-vor-datendieben
http://www.facebook.com/groups/491112987636270/ - Facebook Gruppe „MOBILE SECURITY"
http://www.xing.com/net/enterprisemobi - XING Fachforum „ENTERPRISE MOBILITY"
http://blog.unixweb.de/vpn-server-aufbau-mit-einem-raspberry-pi/

Links zum Thema „CryptoParty":

http://de.wikipedia.org/wiki/CryptoParty
http://www.cryptoparty.in/parties/howto
http://www.youtube.com/watch?v=o9HOf16N0ho

Links zum Thema „Digitale Selbstverteidigung":

https://prism-break.org/#de
http://kryptoparty.de/?page_id=65
http://www.stopwatchingus-duesseldorf.org/tools/
http://demonstrare.de/demonstrare/etwas-mehr-sicherheit-mit-android-linux-und-windows/
http://cybermashup.com/2013/07/24/nsa-crypto-and-bananas/
http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance
http://www.youtube.com/watch?v=N8Sc6pUR1mA
http://www.youtube.com/user/CCCdeVideos

Links zu Apps/Software/Tools/Downloads: ACHTUNG: es werden NICHT alle behandelt !

TEIL 1 – Verschlüsselte eMail-Kommunikation

eMail-Verschlüsselung: OpenPGP / GnuPG / GPG
http://www.gnupg.org/

Android: **APG** (OpenPGP, zusammen mit K-9 Mail)
http://play.google.com/store/apps/details?id=org.thialfihar.android.apg

iOS: **iPGMail** (OpenPGP)
http://itunes.apple.com/us/app/ipgmail/id430780873?mt=8

iOS: **oPenGP** (OpenPGP)
http://itunes.apple.com/de/app/opengp/id414003727
http://itunes.apple.com/de/app/opengp-lite/id405279153

Windows Phone: **oPenGP** (OpenPGP)
http://www.windowsphone.com/de-de/store/app/opengp/449af4e8-d259-431f-b5d9-3ebb092c13d1

Windows: **Gpg4win** (OpenPGP + S/MIME, zusammen mit Microsoft Outlook oder Claws Mail)
http://www.gpg4win.org/

Mac OS: **GPGMail** + **GPG Suite** (OpenPGP, zusammen mit Apple Mail oder Thunderbird)
http://gpgtools.org/

Windows / Mac OS / Linux: **Enigmail** (OpenPGP, zusammen mit Thunderbird)
http://addons.mozilla.org/de/thunderbird/addon/enigmail/

eMail-Programme:

Android: **K-9 Mail** (zusammen mit APG)
http://play.google.com/store/apps/details?id=com.fsck.k9

Windows / Mac OS / Linux: **Mozilla Thunderbird** (Addons/Plugins siehe oben, v.a. Enigmail)
http://www.mozilla.org/de/thunderbird/
http://www.mozilla.org/de/thunderbird/all.html

TEIL 2 - Secure Messaging

THREEMA: Messaging mit End-To-End-Verschlüsselung (ECC mit NaCl)
http://threema.ch/
Android: http://play.google.com/store/apps/details?id=ch.threema.app
iOS: http://itunes.apple.com/de/app/threema/id578665578?mt=8
versus OTR: http://threema.ch/de/faq.html

XMPP + **OTR**: XMPP-Dienste: Facebook Messenger, Google Talk, Jabber, AIM, ICQ, ...
Sichere XMPP-Clients mit OTR-Verschlüsselung:

Android: **Xabber** (XMPP-Dienste > FB, GT, ...)
http://play.google.com/store/apps/details?id=com.xabber.android&hl=de
http://play.google.com/store/apps/details?id=com.xabber.androidvip&hl=de

Android: **ChatSecure** (ehem. Gibberbot; XMPP-Dienste > FB, GT, Jabber, AIM)
http://play.google.com/store/apps/details?id=info.guardianproject.otr.app.im&hl=de

iOS: **ChatSecure** (ehem. Gibberbot; XMPP-Dienste > FB, GT, Jabber, AIM)
http://itunes.apple.com/us/app/chatsecure-encrypted-secure/id464200063

Windows / Mac OS / Ubuntu / Linux: **Pidgin** plus **OTR-Plugin**
http://www.pidgin.im/download/
http://developer.pidgin.im/wiki/ThirdPartyPlugins
http://otr.cypherpunks.ca/index.php#downloads

Windows / Mac OS / Ubuntu / Debian / Linux: **Jitsi**
http://jitsi.org/Main/Download

Verschlüsselte SMS/MMS:

Android: **TextSecure**
http://whispersystems.org/#encrypted_texts
http://play.google.com/store/apps/details?id=org.thoughtcrime.securesms

iOS: **TextSecure** (in Entwicklung)
http://whispersystems.org/blog/iphone-rsn/

TEIL 3 - Verschlüsselte Sprachkommunikation / Telefonie

OSTel (Open Secure Telephony des Guardian Project): Encrypted SIP Service Provider
https://ostel.co/
(Achtung: VoIP lässt nicht jeder Mobiltelefon-Provider bzw nur bei bestimmten Tarifen zu, Alternative: über WLAN)

CSipSimple: (VoIP-Client, Nutzung z.B. mit Encrypted SIP Dienst wie OSTel)
http://code.google.com/p/csipsimple/
Android: **CSipSimple**
http://play.google.com/store/apps/details?id=com.csipsimple
http://nightlies.csipsimple.com/stable/CSipSimple-latest-trunk.apk

iOS: **Acrobits SoftPhone** (VoIP-Client, Nutzung z.B. mit Encrypted SIP Dienst wie OSTel)
http://itunes.apple.com/app/acrobits-softphone-sip-phone/id314192799

Android: Acrobits **Groundwire** (SRTP: SDES + ZRTP)
http://www.acrobits.cz/94/groundwire-for-android
http://play.google.com/store/apps/details?id=cz.acrobits.softphone.aliengroundwire
iOS: Acrobits **Groundwire** (SRTP: SDES + ZRTP)
http://www.acrobits.cz/11/acrobits-groundwire-for-iphone
http://itunes.apple.com/de/app/groundwire-business-caliber/id378503081?mt=8

PrivateGSM (SRTP/ZRTP, SIP/TLS):
http://guardianproject.info/wiki/PrivateGSM
http://www.privatewave.com/display/WS/PrivateGSM
Android: **PrivateGSM Professional**
http://play.google.com/store/apps/details?id=com.privategsm.beta
iOS: **PrivateGSM Professional**
http://itunes.apple.com/de/app/privategsm-professional/id401908184?mt=8

Android: **RedPhone** (ZRTP Encrypted VoIP Channel)
http://whispersystems.org/#privacy
http://play.google.com/store/apps/details?id=org.thoughtcrime.redphone

BlackBerry 10: **SecuSUITE** (SNS-Standard: CSD-Kanal, ISDN V110, SNS over IP)
http://www.secusmart.com/secusuite/
BlackBerry 10: **SecuVOICE** (SNS-Standard: CSD-Kanal, ISDN V110, SNS over IP)
http://www.secusmart.com/secuvoice/
Android: **SecuVOICE** (SNS-Standard: CSD-Kanal, ISDN V110, SNS over IP)
http://www.secusmart.com/secuvoice/android-smartphones/funktionsweise/

Windows / Mac OS / Ubuntu / Debian / Linux: **Jitsi**
http://jitsi.org/Main/Download

TEIL 4 - Gerät / Datenträger / OS / Virtualisierung / Container

Android: **BizzTrust**
http://www.bizztrust.de

Android: **SiMKo3**
http://www.t-systems.de/simko

BlackBerry 10: **BlackBerry Balance**
http://de.blackberry.com/software/smartphones/blackberry-10-os/features-new/blackberry-balance.html

BlackBerry 10: **SecuSUITE**
http://www.secusmart.com/secusuite/

Android / iOS: **Good Collaboration Suite**
http://www1.good.com/applications/collaboration-suite/

Android: Verschlüsselung (des Gerätespeichers) mit Bordmitteln
> Einstellungen > Sicherheit > Verschlüsselung > Gerät verschlüsseln
> Einstellungen > Sicherheit > Verschlüsselung > Externe SD-Karte verschlüsseln

Android: **LUKS** (Encrypted Container, im internen Gerätespeicher oder auf SD-Karte)
https://guardianproject.info/code/luks/
https://play.google.com/store/apps/details?id=com.nemesis2.luksmanager

TrueCrypt: (Festplatten-Verschlüsselung)
http://www.truecrypt.org
Windows / Mac OS / Linux:
http://www.truecrypt.org/downloads

OpenSource **Alternativen** bei mobilen Betriebssystemen:

Ubuntu Phone
http://www.ubuntu.com/phone

TEIL 5 - Collaboration + Cloud-Speicher (verschlüsselt)

Stackfield: Collaboration Plattform mit End-to-End-Verschlüsselung (Freemium)
http://www.stackfield.com

Wuala: verschlüsselter Cloud-Speicher-Dienst
http://www.wuala.com/de/
Android, iOS, Windows, Mac OS, Linux:
http://www.wuala.com/de/download/
Android: http://play.google.com/store/apps/details?id=com.wuala.android
iOS: http://itunes.apple.com/us/app/wuala/id417749289?mt=8

BoxCryptor: Verschlüsselung von Cloud-Speicher
http://www.boxcryptor.com/
Unterstützt Cloud-Speicher-Dienste: Dropbox, Google Drive, SkyDrive, BOX, SugarSync.
Für Android, iOS, Windows RT, Windows, Mac OS X, Linux, Chrome (Browser Plugin):
http://www.boxcryptor.com/de/download
BoxCryptor Classic:
Android: http://play.google.com/store/apps/details?id=com.boxcryptor.android
iOS: http://itunes.apple.com/de/app/boxcryptor-classic/id484546808
BoxCryptor (2.x):
Android: http://play.google.com/store/apps/details?id=com.boxcryptor2.android
iOS: http://itunes.apple.com/de/app/boxcryptor/id649940870?mt=8

TEIL 6 - VPN-Tunnelverbindung

Android: VPN mit Bordmitteln
> Einstellungen > Drahtlos und Netzwerke > Weitere Einstellungen > VPN

iOS: VPN mit Bordmitteln
> Einstellungen > Allgemein > VPN

Windows Phone: unterstützt VPN systemseitig nicht

OpenVPN: http://openvpn.net/
Android: OpenVPN Connect
http://play.google.com/store/apps/details?id=net.openvpn.openvpn&hl=de
iOS: OpenVPN Connect
http://itunes.apple.com/us/app/openvpn-connect/id590379981
Windows: OpenVPN Private Tunnel
http://swupdate.openvpn.net/privatetunnel/client/privatetunnel.msi
Mac OS: OpenVPN Private Tunnel
http://swupdate.openvpn.net/privatetunnel/client/privatetunnel.dmg

ANHANG – Weiterführende Links zum Thema

http://wiki.piratenpartei.de/PGP

http://www.spiegel.de/fotostrecke/openpgp-so-verschluesseln-sie-ihre-e-mails-fotostrecke-98718.html

http://wiki.piratenpartei.de/HowTo_Emails_verschl%C3%BCsseln_mit_PGP_mit_Thunderbird#Installation_und_Ver.C3.B6ffentlichen_der_Schl.C3.BCssel

http://www.verbraucher-sicher-online.de/anleitung/e-mails-verschluesseln-in-apple-mail-unter-mac-os-x?page=0,2#eigenes_schluesselpaar

http://wiki.ubuntuusers.de/GnuPG

http://stadt-bremerhaven.de/android-verschluesselte-e-mails-mit-agp-und-k9-senden-und-empfangen/

http://www.apfeltalk.de/community/threads/eine-anleitung-fuer-die-verschluesselung-von-mails-unter-ios-5.389590/

http://irrsinnig.de/sicher-im-netz/verschluesselt-chatten-mit-otr

http://www.androidpit.de/verschluesselte-sms-chats-textsecure-xabber

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Sicherheitshinweise/2009-07-10_Sicherheitshinweis_GSM_pdf.pdf

https://www.bsi.bund.de/DE/Themen/weitereThemen/MobileSecurity/SNS/sns_node.html

http://idw-online.de/de/news563139