Sun City Computer Club

Cyber Security SIG

January 6, 2021

Questions, Comments, Suggestions welcomed at any time

Even Now



- Audio recording of this session as MP4 file
- Audio recording available at link shown above

Audio Recording In Progress

SIG attendees are required to be members of the chartered club sponsoring that SIG.
Sun City Community Association By-law



5.4. Protocols and Standards to be used for encryption mechanism: s/MIME and related packages

The open standard s/MIME as extension to de facto e-mail standard SMTP will be deployed to encrypt messages containing DNA profile information. The protocol s/MIME (V3) allows signed receipts, security labels, and secure mailing lists and is layered on Cryptographic Message Syntax (CMS), an Internet Engineering Task Force (IETF) specification for cryptographic protected messages. It can be used to digitally sign, digest, authenticate or encrypt any form of digital data.

The underlying certificate used by the s/MIME mechanism has to be in compliance with X.509 standard. In order to ensure common standards and procedures with other Prüm applications, the processing rules for s/MIME encryption operations or to be applied under various Commercial Product of the Shelves (COTS) environments, are as follows:

- the sequence of the operations is: first encryption and then signing,
- the encryption algorithm AES (Advanced Encryption Standard) with 256 bit key length and RSA with 1024 bit key length shall be applied for symmetric and asymmetric encryption respectively,
- the hash algorithm SHA-1 shall be applied.

s/MIME functionality is built into the vast majority of modern e-mail software packages including Outlook, Mozilla Mail as well as Netscape Communicator 4.x and inter-operates among all major e-mail software packages.

Cyber & Legislation



- Windows 0-day CVE-2020-0986 fix broke
- Azure/Microsoft 365 malicious activity tool
- Adobe Flash end
- Y2K "fix" 1990 1920 => 2000 2020
- Zyxel backdoor
- Smart home devices swatting
- T-Mobile data breach
- Ticketmaster \$10M fine
- Restricted folder access
 Brute Forcing Antivirus

Current Issues



Google Chrome 87 secure form warning



Actually post-submission redirect

Current Issues



- Browser cache wars
- Kazakhstan root certificate
- Ransomware Task Force
- CVE-2021-3021 as of Jan 5
- BSSID to geo-to-BSSID
- Telegram "People Nearby"

Current Issues



iMessage 'Data Linked To You'

- Contact Info
- Email Address
- · Phone Number
- Search History
- I Identifiers
- Device ID

WhatsApp 'Data Linked To You'

Analytics

Purchases

Purchase History

◀ Location

Coarse Location

Contact Info

Phone Number

User Content

Other User Content

Identifiers

User ID Device ID

Usage Data

Product Interaction Advertising Data

Diagnostics

Crash Data Performance Data Other Diagnostic Data

App Functionality

Purchases

Purchase History

Financial Info

Payment Info

◀ Location

Coarse Location

Contact Info

Email Address Phone Number

Contacts

Contacts

User Content

Customer Support Other User Content

DB Identifiers

User ID Device ID

Usage Data

Product Interaction

Diagnostics

Crash Data Performance Data Other Diagnostic Data

WhatsApp



- Hardware model
- Operating system
- Browser info
- IP address
- Mobile network info
 Phone number, etc.

WhatsApp metadata



Signal 'Data Linked To You'

Message 'Data Linked To You'

O lease on. @ naviron a framework 2 ---a Proportional 1 between

WhatsApp

designer. · Perriese * Literature · Damester The second second Star brief Albert Stemphology OR Intelligen

200 15

all time bes

@ Deposite

Broader Harry Sells

Strick Stage and Street

'Data Linked To You'

AN THEOTomates · Parties

· Innecessor W.Lessen

OF CHICAR PRO-That half-our Si Contario

Mit Law Sorter 6 Office or second

the contract 100.0

off I temper from

O Treatment Transcribed Operations of Balls Facebook Messenger 'Data Linked To You'

· Purmann

Henry Inc.

₱ totales

The finance of

· Turnesi

The other patients and a selection

the residence of books

· Demonsor Time Helius -

Transport Control il commo 1000000

OR THE TANKS Total States Committee

@ least heavy September 1

manufacture (Co.

ptd in ougs being

· ingenter

TOTAL PROPERTY.

Street See

China Sala Sano

and the last last

the Same In

Bridge & Transport Street Same · management (Compression) Mil Herrison

M. Sant Street payment House, · Innerty Henry

O male a reason

mark.

· Perform

68 Streemed Select

T bearing

Denne who

Total Pro-

-

@ famous

B contract

Spine (II)

M months. -

All trapping Print of Contractions

de lamateur etc. .

· improve (New York)

S live bee Self-Self-Sensor Peoble Demonstration tea Protetteration

> O reach & freeze Frank.

· Punitere III Francis on

· Committee Practice service. No. John pays Lamber His

& comery (comment) Mineral Control and the sense of

d seen many

Marine march · management Statement Statement SE morror

Acres 61 of the law

married to be a second O Senterio

> 1904,004,000 @ Neprotity PD4 Ned Management later

· Direction

· Servetina belo

B Transie ----

· Other State

Stilled Properties

· Trichest

OR Transport * ---

Exist the

-

.

declaration for the second

III receive ---

pit Design have

· Programme

SHEET THE RESERVED

100-040

Section Street

· Derivativity Roser States Inde-States

₹ Leuten To the last O Constitution & tenor

PRINCIPAL ARRIVATION THE RESERVE Mill Steel Control -

di Common . the term benefit · insert inner.

the case to serve Photo of Males

Of Sections Street dearer

@ Descriptions: demand in chance, -

100 self-times have

----· involve desprise have



- WAY more than initial reports
- Cloud providers AWS & Microsoft
- Microsoft source code
- SolarWinds source code Eastern Europe
- Servers inside US, NSA can not protect Einstein did not detect
- Election defense diversion
- Early warning sensors not tripped
- October 2019 Deliberate delay
- Widely deployed Trusted Exempt
- Espionage
- ALTER ?

SolarWinds updates



- FireEye Red Team tools
- Timing? Pandemic, Government transition, WFH
- Follow on Backdoors
- Asymmetric response
- Backdoor removal
- Signed how so?
- Build dll in memory SuperNova
- Second threat actor?
- Hide in printer, camera, etc.
- And CVE-2020-10148
- US intelligence formally accuse Russia

SolarWinds Update



- NotPetya Russia Ukraine wiper tax app
- Cisco, disk manufacturers, security devices
- Ccleaner

Supply Chain attacks



- OPM
- F35
- Covid

Espionage



<u>Uninstall Flash Player for Windows</u> (adobe.com)

https://helpx.adobe.com/flash-player/kb/uninstall-flash-player-windows.html

Adobe Flash





- Helpful < > Harmful
- Awareness, Preparedness, Understanding

Computer Club, Help Center, SIGs, Presentations, FirstTime, classes Cyber Security SIG meetings, NEWSBLOG Internet

• Questions, suggestions, comments?

SCCCCyber@gmail.com

