# Sun City Computer Club

Cyber Security SIG

January 6, 2021

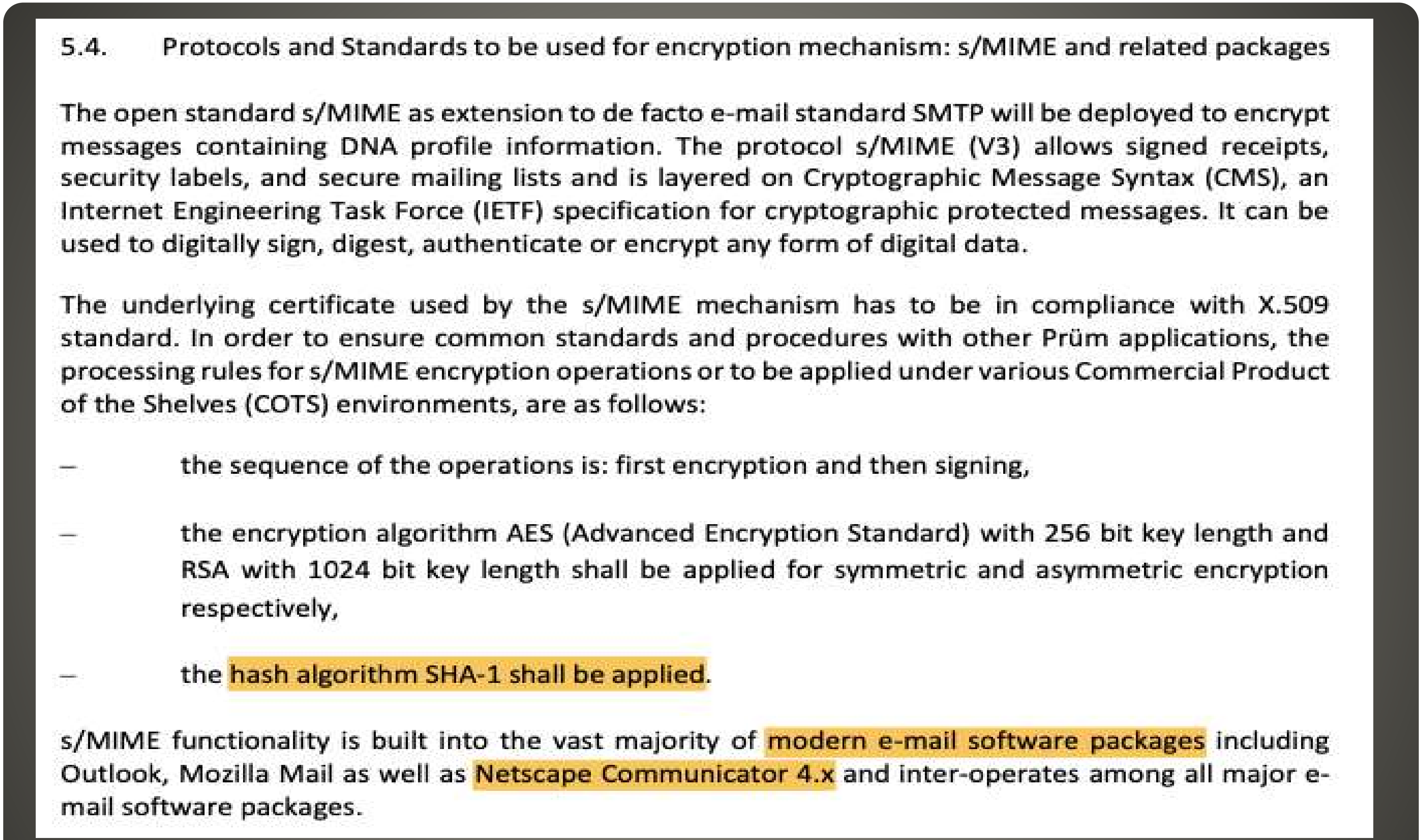
**Questions, Comments, Suggestions welcomed at any time**

**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

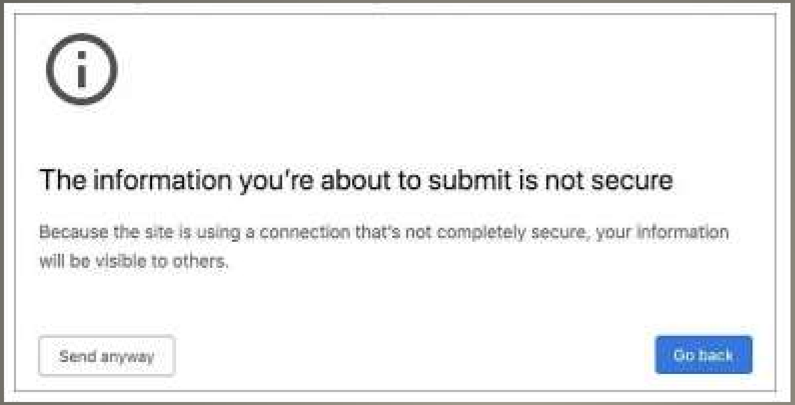
# Current Issues

- 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



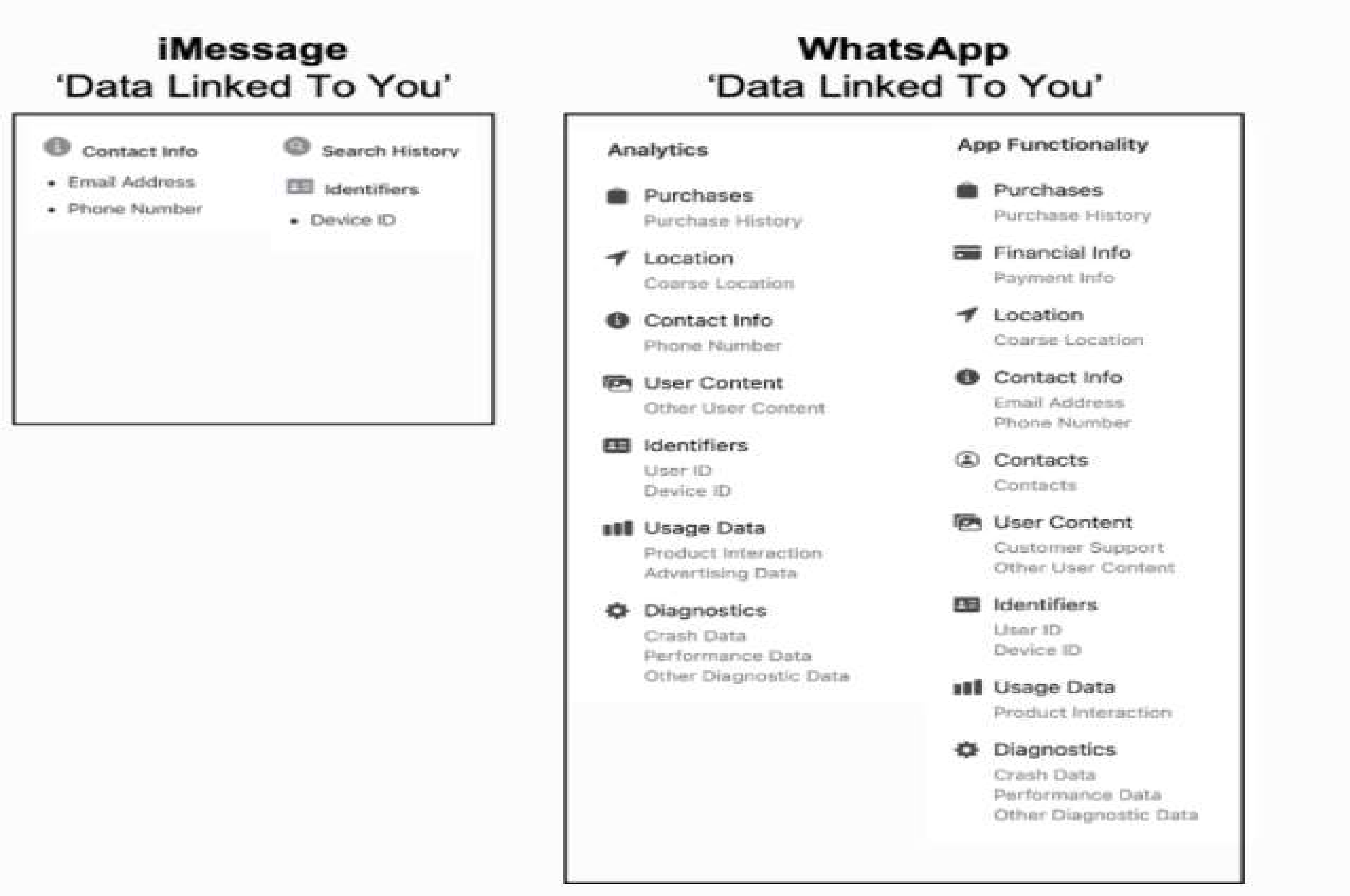
The information you're about to submit is not secure

Because the site is using a connection that's not completely secure, your information will be visible to others.

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”



**iMessage**
**'Data Linked To You'**

- Contact Info
  - Email Address
  - Phone Number
- Search History
- 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**

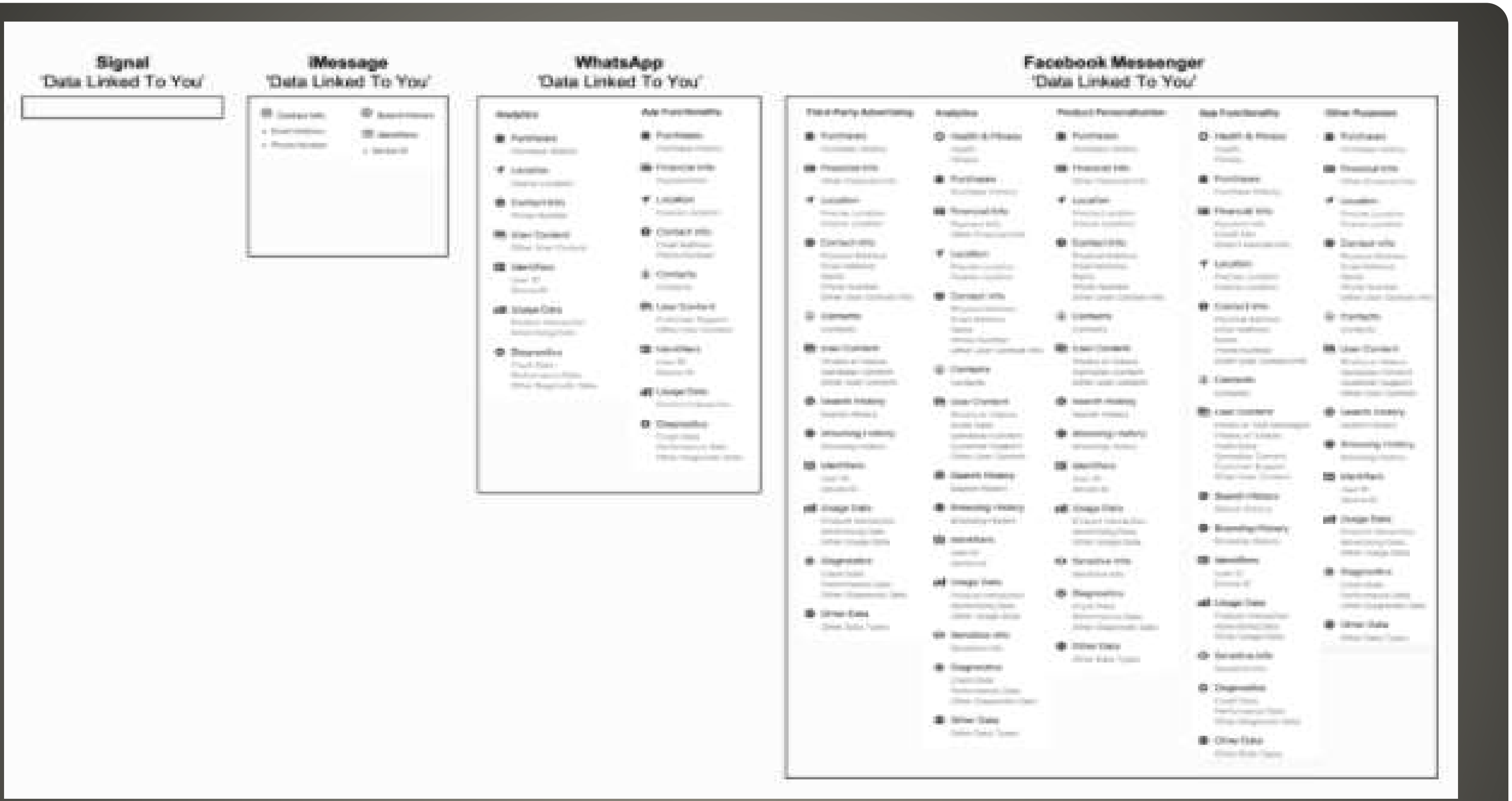
- Purchases
  Purchase History
- Financial Info
  Payment Info
- Location
  Coarse Location
- Contact Info
  Email Address
  Phone Number
- Contacts
  Contacts
- User Content
  Customer Support
  Other User Content
- Identifiers
  User ID
  Device ID
- Usage Data
  Product Interaction
- Diagnostics
  Crash Data
  Performance Data
  Other Diagnostic Data

# WhatsApp

# WhatsApp metadata

- Hardware model
- Operating system
- Browser info
- IP address
- Mobile network info

  Phone number, etc.



Signal
'Data Linked To You'

iMessage
'Data Linked To You'

WhatsApp
'Data Linked To You'

Facebook Messenger
'Data Linked To You'

# SolarWinds updates

- 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 Update

- 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

# Supply Chain attacks

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

# Espionage

- OPM
- F35
- Covid

Uninstall Flash Player for Windows (adobe.com)

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

# Adobe Flash

QUESTIONS ?

- 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**