Silex Webinar:
Everything You Need to Know About California's New Cybersecurity Legislation

Tuesday, December 10, 2019

silex technology

Speakers

Babar Hashim
Senior Product & Marketing Management
Silex Technology America

Zac Freeman
VP of Sales & Marketing
Silex Technology America

Who we are

When it **Absolutely Must** Connect

Connectivity Technology Provider

Established in 1973

Headquarters near Kyoto, Japan

15 Year Qualcomm ADC Partner

Embedded Wireless

Device Connectivity

Wireless Infrastructure

Display Connectivity

WHEN IT ABSOLUTELY MUST CONNECT.

Successful connectivity solutions include the premium hardware and software supported by the right compliance and certifications.

HARDWARE

- 802.11n, 11ac, 11ah, 11ax, 11ad, Bluetooth, 802.15.4
- IoT, SDIO, PCIe, USB, SPI/UART, Ethernet interfaces
- End Product, Subsystem, Module, SiP
- Full custom/modified standard manufacturing

COMPLIANCE

- FCC/IC/CE/MIC
- Global Certifications
- IEEE 802.11
- Quality
- RoHS/REACH
- Cybersecurity

SOFTWARE

- Linux, Android, Windows, Free RTOS, MQX, Greenhills, VxWorks
- WPA2 PSK, Enterprise, CCX security, FIPS
- Fast roaming, mesh networking, low latency, provisioning, regulatory test, logging and diagnostics tools
- Development environment and SDK
- Custom BSP, driver and application development

silex technology

I am NOT a lawyer!

silex technology

The First State to Regulate

Timeline:

September 28th, 2018 the California Governor, Jerry Brown, signed into law two, almost identical, bills:

(1) Senate Bill No. 327

(2) Assembly Bill No. 1906

Intent:

Have manufacturers of connected devices equip them with reasonable security features appropriate to the function of the device to prevent unauthorized access, destruction, use, modification or disclosure of information contained in the device.

silex technology

2018 California Code
TITLE 1.81.26.a - Security of Connected Devices
Section 1798.91.05.

Authentication:

A method of verifying the authority of a user, process, or device to access resources in an information system.

Connected Device:

Any device, or other physical object capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address.

Manufacturer:

The person who manufactures, or contracts with another person to manufacture on the person's behalf, connected devices that are sold or offered for sale in California. For the purposes of this subdivision, a contract with another person to manufacture on the person's behalf does not include a contract only to purchase a connected device, or only to purchase and brand a connected device.

Security Feature:

A feature of a device designed to provide security for that device.

Unauthorized access, destruction, use, modification, or disclosure:

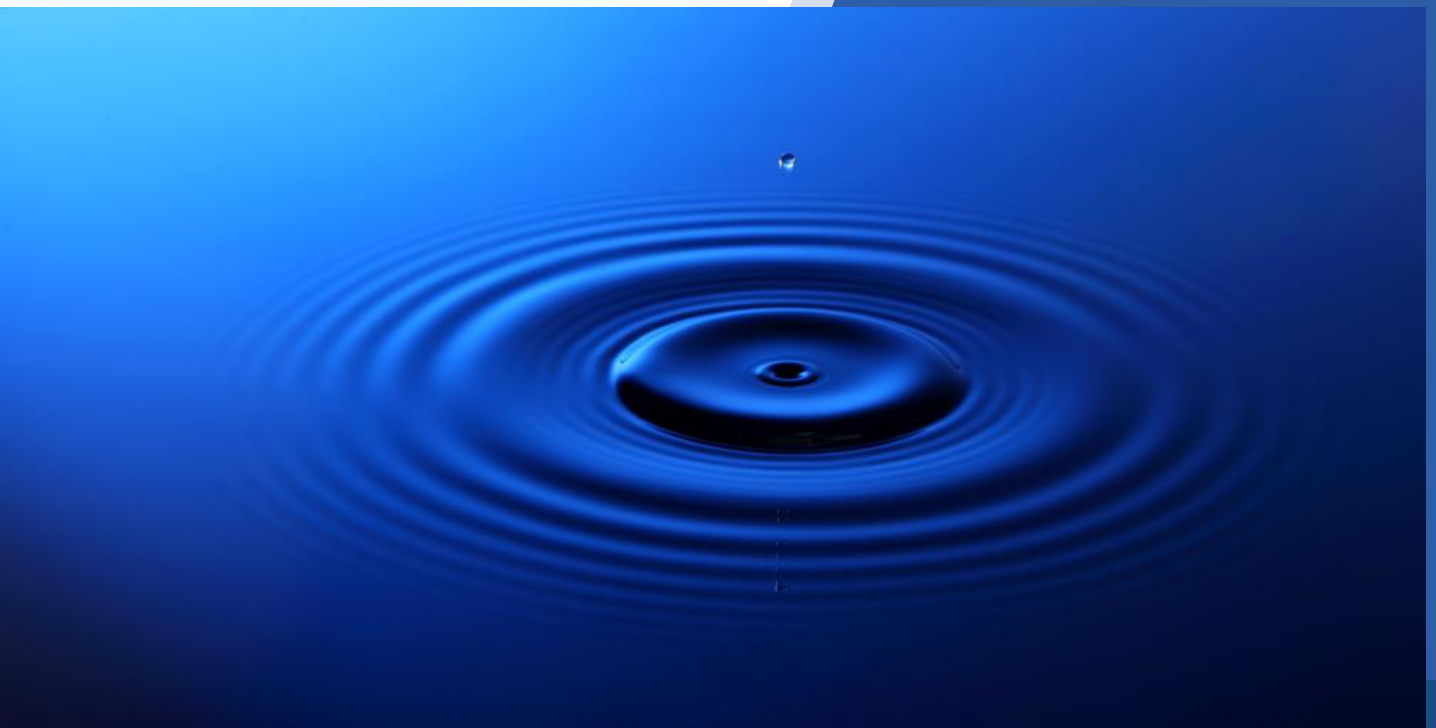
Access, destruction, use, modification, or disclosure that is not authorized by the consumer.

silex technology

Who Will Feel the Impact?

Manufacturers

Any manufacturer of a communications devices that connects to an IP network that may, directly or indirectly, connect to the internet that contain a network accessible control/access interface.



Devices

End point devices:

Laptops, desktops, cell phones, tablets, IoT (cameras, voice assistants, thermostats, etc.)

Network Infrastructure:

Access points, routers, switches, hubs, WLAN controllers, etc.

Connectivity Devices:

Ethernet client bridges, USB bridges, serial bridges, etc.

Easy Password Access

- A simple password is universally used by communications equipment manufactures to make initial configuration easy.

- Examples:
  - Linksys: admin
  - Dlink: admin
  - TPLink: admin
  - Cisco: cisco

The Problem with Default Passwords

Default Password Intent: The idea is that one of the first steps would be for the consumer to change the default password to a unique password only to them

The Reality: The default password change does not happen in most cases.

Security Threats: Anyone, cybercriminal or not, searching the network can find the equipment and easily identify the manufacturer and default authorization requirements, subsequently gaining accessing to the equipment.

silex technology

Implementing Reasonable Security

Reasonable security must be provided through modification of the derivation of the device credentials using one of two proposed methods:

1

A unique password for every device shipped (as identified specifically in the bill)

2

Force the consumer to create unique authentication credentials during the initial set up of the device.

silex technology

Method 1: Unique Credentials

Pros

- This is potentially very strong solution as no two devices shipped would have the same password
  - Difficult for intruder to find the password

Cons

- Logistics of installing a unique password
  - Every shipped unit is different
- Providing access to the unique password
  - On product vs. manual vs. on-line
- Recovery of lost unique password

Method 2: Forced Credentials

Pros

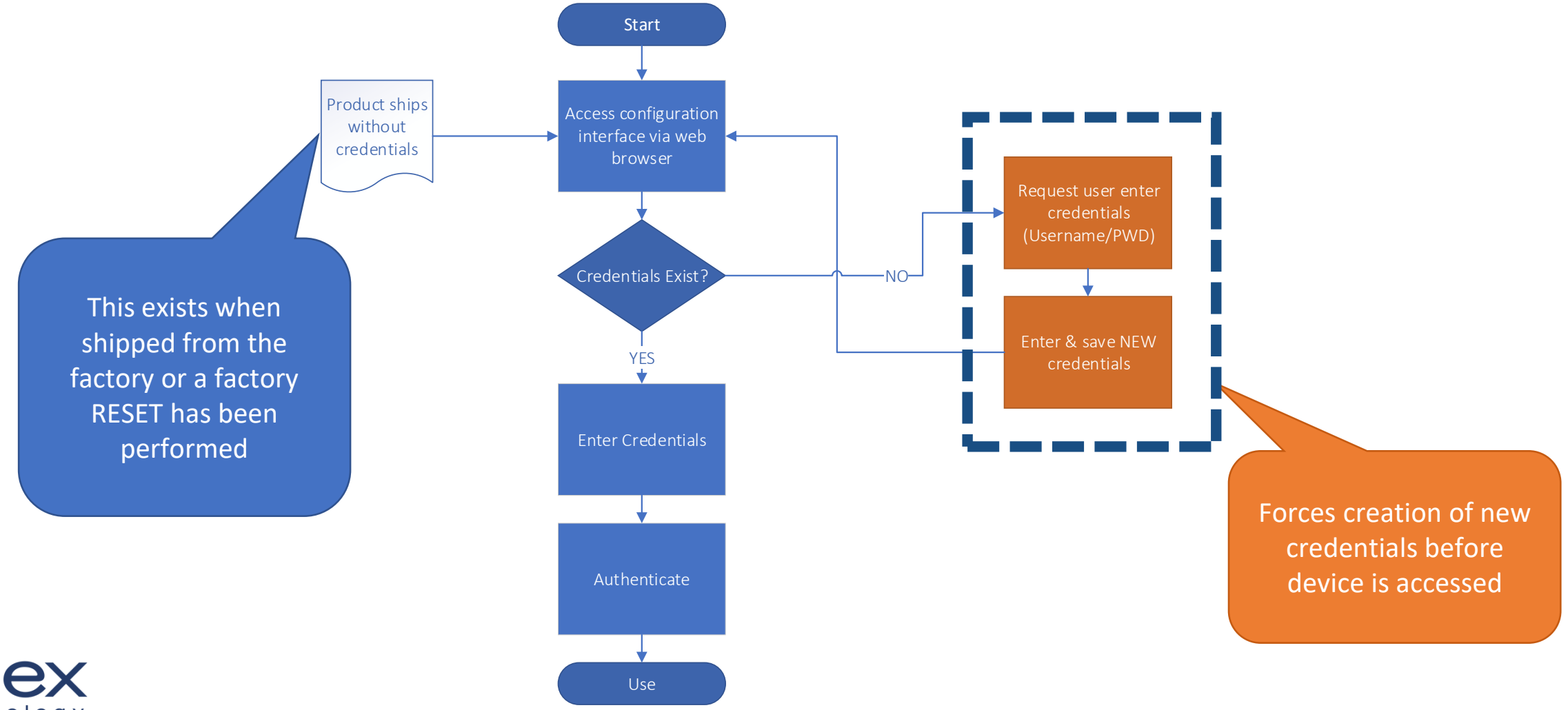
- Simplifies logistics for product manufacturing
  - All products are the same
- Forces creation of secret credentials
- Method for recovery from lost credentials
  - Factory RESET

Cons

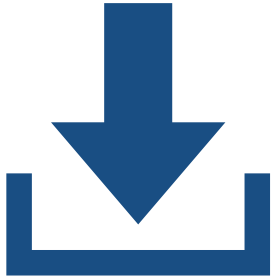
- Strength of credentials questionable
  - Unless check is part of process
- Uniqueness of credentials is not guaranteed
  - Possible reuse

Silex's Plan of Action

Method 2: Forced Initial Credentials



Silex's Plan of Action Continued…..

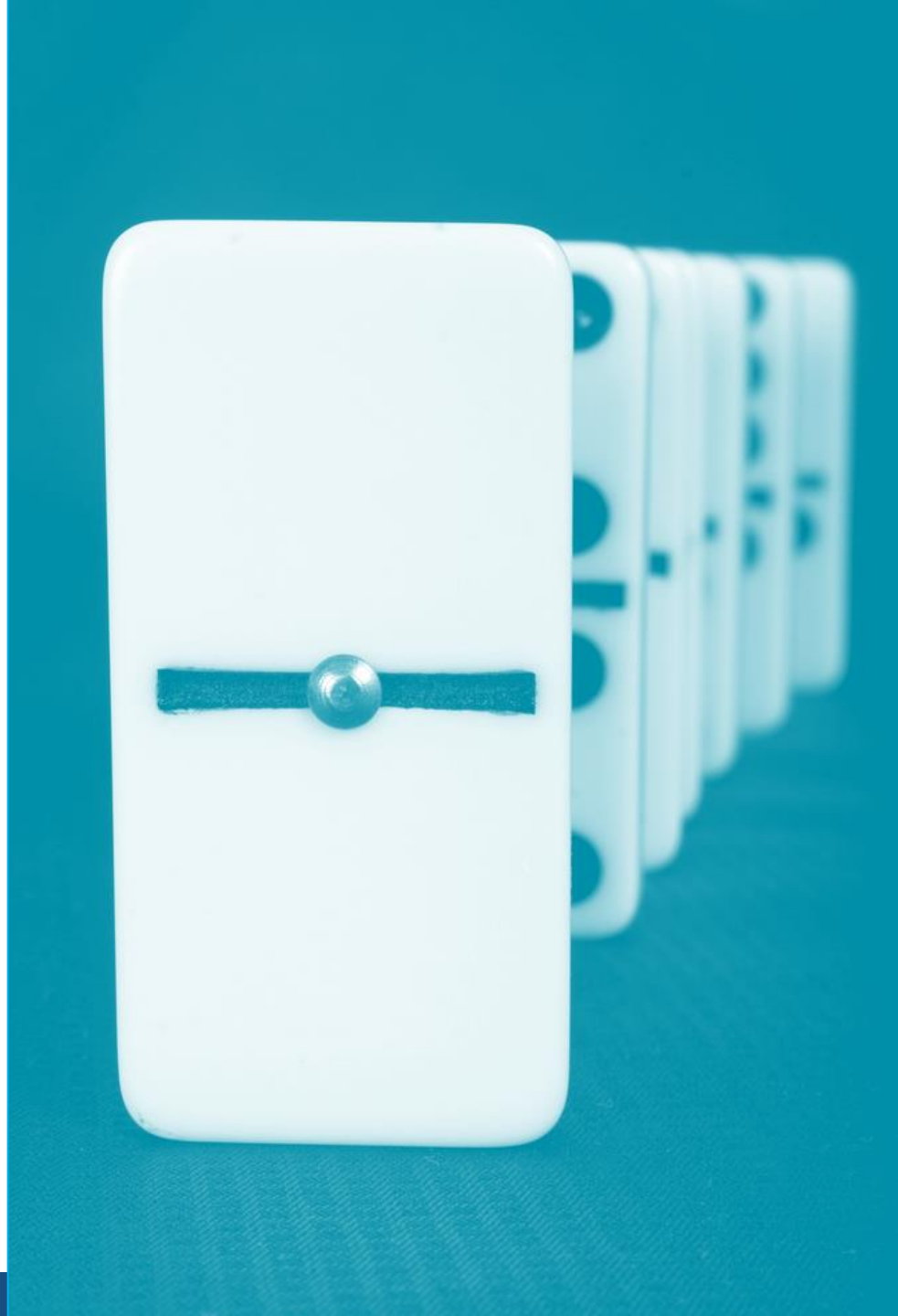


Update via firmware download and update

After update you will require new credentials

Impacted Products:

Product Family	Part Number
Intelligent Module	SX-590
Bridge	BR-300AN BR-310AC SX-BR-4600WAN2
Access Point	SX-AP-4800AN2 AP-500AC AP-415AN
Device Server	DS-510 DS-520AN DS-600 SD-300 SD-330AC SC-400ACL
Mesh	BR-400AN MNS-300EM



silex technology

Market Exceptions

Federally Regulated Devices

Medical devices

Looking Into the Future

- There is no explicit or implied penalty described in the bill
- The legislation does not enable a direct path for action from the consumer
- It is not clear the timing jurisdiction as there is no specific guidance on the effectivity of the Jan 1st, 2020 date with respect to products already in inventory
- The recent introduction of CCPA (California Consumer Privacy Act) may intersect and piggy-back with the bills
    - The recommendation is that manufacturers should consider how the compliance efforts for all privacy regulation may overlap and impact decisions

silex technology


Q&A


thank you
danke
謝謝
ngiyabonga
рахмат
teşekkür ederim
спасибо
gracias
tapadh leat
dank je
obrigado
dziękuję
bedankt
go raibh maith agat
merci
sukriya
kop khun krap
terima kasih
dakujem
arigatô
grazie
takk
taiku
sagolun
maururu
hvala
dhanyavad
kiitos
dankie
nanni
nandri
köszönöm
bayarlalaa
gràçie
enkosi
Баярлалаа
faafetai lava
vinaka
спасибі
blagodaram
mersi
kia ora
barka
welalin
tack
spas
misaotra
matondo
paldies
grazzi
mahalo
хвала
asante
manana
obrigada
tenki
murakoze
chokrane
djiere dieuf
tau
mochchakkeram
mamnun
дякую
chnorakaloutioun
gratias ago
gràcies
sulpáy
akun
dankon
ačiū
sobodi
děkuji
mèsi
didi madloba
najis tuke
kam sah hamnida
rahmat
ありがとう
tanemirt
rahmet
diolch
ευχαριστώ
xièxie
감사합니다
তোমাকে ধন্যবাদ
dhanyavadagalu
shukriya
mercé
мерси
trugarez