OUTLINE

- What is a Smart Device?
- Smart device Penetration in Ghana
- What are Ghanaians doing on smart devices?
- Risk to the Corporate
- Controls
- Conclusion
WHAT IS A SMART DEVICE?
What is a Smart Device?

- An electronic device generally connected to other devices or networks via different protocols such as Bluetooth-NFC-WiFi-3G-etc. that can operate to some extent interactively and autonomously (Collins Dictionary)
- A device programmed so as to be capable of some independent action (Oxford Dictionary)
- Eg. Phones, Tablets, Tv etc
Smart device Penetration in Ghana

- An International Telecoms Union report ranked Ghana as the first in Africa with more people using or connected to mobile broadband.
- An estimated 16m mobile phones are used in this country with 25m citizens, with many owning more than one SIM card.
- A Telecoms Analyst attributed Ghana’s outstanding international rating in mobile broad-band penetration to the increasing use of smart-phones in the country.
WHAT ARE GHANAIANS DOING ON SMART DEVICES?
What are Ghanaians doing on smart devices?

- Social Media
- Downloading Apps for varied purposes
- Browsing
- Accessing Corporate emails
- File movement (as usb sticks)
- Mobile Banking / Mobile Money
RISK TO THE CORPORATE
Risk to the Corporate

- Social Media/Apps/File movement/Browsing
  - A typical corporate network has a Firewall, Spam filters, IDS/IPS, Proxy Servers to secure the network
  - A user using a smart phone has access to the internet via a telco whose internet usage policy is not the same as the corporate
  - Plugging in the phone to the usb port of the corporate PC exposes the corporate if the phone has been compromised
Risk to the Corporate

- Accessing Corporate emails
  - Risk of data leakage resulting from device theft or loss
  - Unintentional disclosure of data due to phone functionality
Risk to the Corporate

- Mobile Banking / Mobile Money
  - Bearer channel
  - Interaction with the Bank
Bearer channel

- SMS Banking

Base Station  Base Station  Mobile Operator  Bank
Bearer channel

- IVR, USSD

- Data carried within the communication layer is not itself encrypted.
Bearer channel

- J2ME, WAP, S@T

- Session encrypted by GSM communication layer and then banking website
- Similar threat as internet banking
J2ME, WAP, S@T

- J2ME uses same channel as WAP
- Have additional security on the app on the handset hence data entered in app can be encrypted
- Consumer needs to establish that the application is being downloaded from the correct source
- S@T is the most secured
- Bank loads its own encryption keys onto the SIM card with the bank’s own developed application
consumer’s data can be stored on the SIM Card and the consumer can be authenticated on the handset prior to having to carry any data across the mobile network.

The data is also encrypted prior to leaving the handset and only decrypted using the bank’s encryption keys within the bank.
Interaction with the Bank

- **SOAP** (*Simple Object Access Protocol*) Or **REST** (*Representational State Transfer*)?

- **WS-Security** - While SOAP supports SSL (just like REST) it also supports WS-Security which adds some enterprise security features.

- **WS-AtomicTransaction** - Need ACID Transactions over a service, you’re going to need SOAP. While REST supports transactions, it isn’t as comprehensive and isn’t ACID compliant.

- **WS-ReliableMessaging** - SOAP has successful/retry logic built in and provides end-to-end reliability even through SOAP intermediaries.
CONTROLS
Controls

- When charging your phone in a corporate environment, put it off.
- Security awareness training
- Use S@T as the bearer channel for your mobile banking as much as possible
- Use SOAP with WS-Security implemented on integration with telcos that requires sensitive transactions
Conclusion

- Smartphones are an incredible tool for a whole range of people and their use will proliferate. However, smartphone security is lagging ten years behind the growth curve, especially as they are so easily lost or stolen.

- Smartphones carry with them the risks of any computer on a network and at the same time cross the divide between voice and data, which brings security risks of its own. For an organization to remain secure, smartphones need to come within the sphere of the security policy, their use needs to be regulated and active steps should be taken to employ them securely.
THANK YOU