Fraud and Data Exfiltration: Defending Against the Mobile Explosion

Aaron Turner

N4STRUCT

Randy V. Sabett

ZwillGen PLLC

Session ID: LAW-401

Session Classification: Intermediate

RSA CONFERENCE 2012

Introductions

- Aaron Turner
  - Partner at newly-formed Security Consultancy

    N4STRUCT

- Randy V. Sabett, J.D., CISSP
  - Counsel at the Boutique Law Firm

    ZG ZwillGen PLLC

Disclaimer (you HAD to be expecting this…)

- Nothing we discuss today constitutes legal advice. For any specific questions, seek the independent advice of your attorney.

Premise & Format

- Aaron will play the role of a Fortune 500 CIO
  - ~10,000 employees spread across 12 countries
- Randy will play the role of outside counsel
  - Will say 'it depends' a lot

- Role play will revolve around two issues:
  - Company is facing increased costs associated with SMS fraud on company-liable mobile service subscriptions
  - Anecdotal evidence that increasing amounts of corporate data are flowing through mobile networks cross-connected to the corporate network

Specific Case 1

- Internal audit controls flagged last quarter's payments to mobile service providers as 130% of planned expenditures
  - Audit team informed technology procurement
  - Technology procurement team manually reviewed billing statements
  - Review resulted in finding 1000's of premium international SMS messages sent from company-liable accounts

Specific Case 2

- 4G WiFi router observed in Guangdon, China offices
  - WiFi monitoring equipment detected presence of WPA-protected signal in/near company office space with the SSID of CARRIER-4G-0254
  - Despite multiple physical search attempts, device has not been located

Specific Case 3

- Abnormal 2G reception reported by users at US Headquarters offices
  - Previously, GSM phone users had seen excellent 3G coverage
  - Beginning about 90 days ago, users started noticing 2G coverage throughout the building
  - Significant data synchronization errors noticed at Mobile Synchronization Gateway for users with mobile devices at US HQ

Case 1:
International Service Fraud

Monitoring International Service Fraud

- Requires some sort of audit function on company-liable lines of service
  - Usually manifests itself as a premium service charge on the monthly statement
- How it happens
  - User gets a TXT that says ‘You’ve been selected as a candidate to get a special incentive from <COMPANY> - reply to this message for more details’
  - Reply-to SMS # is formatted as something like

    +97285412314

    (if HQ is in Dallas for example)
- Financial impact
  - Some Premium-rate SMS responses can charge up to $10 per message depending on Carrier controls/agreements

CIO Gets the Bill – Potential for Claw-back?

- Over the last 90 days CIO gets report of $12,500 in international premium service charges
  - Initial investigation appears to have uncovered a targeted SMiShing campaign asking users to register for a corporate pilot program

    "+97225846548: Reply now to be eligible for COMPANY's iPad2 pilot program"

  - 1000's of users affected, but difficult to quantify precisely how many targeted beyond BES-connected users
  - Perpetrators appear to have a comprehensive list of company-associated mobile #'s (copy of the GAL?)
- What potential for Claw-back is there for Company with Carriers?

Attorney lays out the SMiShing options

- No laws covering this type of attack (yet)
  - Even if there were, would mostly focus on consumer
- In a commercial setting, most recourse questions will come down to the contract
  - Does the K address fraudulent use of carrier network?
  - What about the SLA?
  - Can company report SMiShing? If so, any recourse?
- Think about all of these PRIOR to provisioning!!
- Also, don't forget about putting SMiShing in your training program

Case 2:
Rogue 4G WiFi Hotspot

State of 4G/WiFi monitoring

- Fairly mature technologies available for WiFi monitoring
  - Very few organizations that are enforcing WiFi security policies
- VERY immature technologies available for enterprise 4G monitoring
- Explosion of low-cost, high-speed personal WiFi devices with 4G capabilities
  - For the price of a monthly home high-speed internet connection, people can take their internet with them wherever they go
- Real-world Impact
  - In 5 Fortune 500 firms last year, 100's of 4G devices detected all over the world

CIO gets an incident report

- Business group has been informed that much of their intellectual property has been found on open-source sites
  - Root cause analysis of network flows traced significant data flows to 3 individuals in the group
  - Additional investigation from HR reveals that those 3 are all leaving the company for various reasons
  - WiFi monitor logs show ‘MiFi-esque’ SSID in the area of the 3 employees
  - Employment-law action underway
- Are there technology options to monitor for this in the future?

4G MiFi detection options

- WiFi detection is very mature
  - Detailed reporting options
  - Most organizations do not have the maturity/culture to take automated action upon detection
- MiFi's can be tethered, thereby avoiding the WiFi detectors
  - What do you do to find a tethered 4G device?
    - USB device policies?
    - Bluetooth restrictions?

- The root cause is 4G
  - We have not seen enterprises with 4G detection capabilities deployed for real-time reporting
  - Monitoring technology exists, but vendors are anxious at letting it loose to enterprises

Attorney lays out the 4G options

- Aaron called it – for this one I’m going to use the ol’ fallback of “it depends”
- There’s that pesky 18 U.S.C. §§ 2510 (ECPA) that prevents eavesdropping, BUT there are exceptions (some of which depend on the role):
  - Consent – most important one in an enterprise setting
  - Safety – “activity which is a necessary incident to the rendition of [the] service or to the protection of the rights or property of the provider of that service”
- Hate to say it, but again back to the contract (in this case the original employment contract)

Case 3:
2G Service Anomalies

Mobile service anomalies at US HQ

- For the last 90 days, users have seen significant service degradation
  - Poor data service and many dropped calls
  - Mobile device synchronization logs show many failed sync attempts
- 2G service degradation – integrity indicator?
  - 3G is hard to crack, so all mobile service hackers force a service downgrade to 2G and then intercept the traffic
  - Most hackers-for-hire do not have the equipment necessary to handle all of the TCP/IP that is flowing through, resulting in significant GPRS/EDGE protocol errors which then cause strange TCP/IP traffic
- Information Security impact
  - Most 2G security incidents are voice/SMS driven

Can a CIO even monitor voice/SMS integrity?

- Technology is available to monitor cellular integrity, but has not been deployed by enterprises
  - Can an enterprise monitor licensed radio spectrum?
- What new paradigms will emerge based on mobile communications integrity challenges?
  - Can an enterprise ‘own’ the spectrum within their building? On their property?

Attorney lays out the 2G integrity options

- Similar to 4G use case – ECPA generally prevents monitoring of these kinds of signals but can look to exceptions
  - Consent
  - Safety
- Ownership of spectrum a remote possibility but few companies likely can pursue this under the current procedures

BUT WAIT A MINUTE!?!?...

What to do now

Immediate action items

- Initiate a mobile service audit
  - Invest in a mobile service billing platform
  - Negotiate premium rate service controls with carriers
  - Make employees aware of SMiShing risks
- Design a ‘MiFi’ controls plan
  - WiFi controls
  - Tethering controls
- Engage legal to do a contracts audit
- 4G/2G controls…
  - Stay tuned – lots happening in the next 12-18 months

Contact info

- Aaron Turner
  aaron.turner@n4struct.com
  www.n4struct.com
  @integricell

- Randy Sabett
  randy@zwillgen.com
  www.zwillgen.com
  blog.zwillgen.com