CSRIC

Communications Security, Reliability and Interoperability Council

Steering Committee

Working Group 2A

Cyber Security Best Practices

March 14, 2011

Presented By: Phil Agcaoili, Co-Chair
Gary Toretti

Executive Summary

❑ A refresh of the 2004 Network Reliability and Interoperability Council (NRIC) Cyber Security Best Practices (187)

❑ Working Group 2A structured into 5 vertical subgroups (Wireless, IP Services, Network, People, and Legacy Services) and 4 horizontal subgroups (Identity Management, Encryption, Vulnerability Management, and Incident Response)

❑ 397 Cyber Security Best Practices from Working Group 2A for 2011 (41% of the 397 are new, 41% are modified NRIC VII best practices, and only 18% of the NRIC VII best practices remained the same)

❑ Service Providers, Network Operators, and Equipment Suppliers are encouraged to review and implement these Cyber Security Best Practices

Working Group Participants

Co-Chairs:
Ed Amoroso – AT&T
Phil Agcaoili – Cox Communication

WG Members/Participants:
Rodney Buie – TeleCommunication Systems
Uma Chandrashekhar – TeleCommunication Systems
Doug Davis - CompTel
Martin Dolly – AT&T
Rob Ellis - Qwest
Fred Fletcher - ATIS
Chris Gardner - Qwest
Bill Garrett - Verizon
Rajeev Gopal – Hughes Network Systems
Allison Growney – Sprint Nextel
Barry Harp – US Department of Health & Human Services
Maureen Harris – NARUC
Robin Howard – Verizon
Dan Huley – Department of Commerce

John Knies – CenturyLink
Micah Maciejewski – Sprint Nextel
Ron Mathis - Intrado
Brian Moir – E-Commerce Telecom Users Group
Jim Payne – Telecordia Technologies
Doug Peck – CA 911 Emergency Comm Office
John Rittinghouse – Hypersecurity LLC
Remesh Sepehrrad – Comcast Corporation
Monique Sims – L.R. Kimball / National Emergency Number Assoc.
Ray Singh – Telecordia Technologies
Jeremy Smith - L.R. Kimball / National Emergency Number Assoc.
Myrna Soto – Comcast Corporation
Julie Tu – FCC Representative

WG Member / Coordinator: Gary Toretti – AT&T

Problem / Deliverable

Problem

- Rapidly evolving and complex technologies in the communication industry are increasingly under attack from insiders, hackers, cyber criminals, and nation-states seeking economic advantage. Compromised technology or process controls can severely impact a company' brand and prowess impacting financials and shareholder value for many years.

Deliverable

- Updated Cyber Security Best Practices reflective of the current technology environment within the Communications' Industry, and related references

Methodology

Wireless (1)	IP Services (2)	Network (3)	People (4)	Legacy Services (5)
WIFI Bluetooth Mobile Devices Mobile Devices Application Security Emerging Devices Wireless 3G, 4G, Microwave, & Satellite	**Broadband Cloud Computing IPV6 Voice over IP**	**Access Control Availability Confidentiality Integrity Security Mgmt Security Audit & Alarm Security Policy & Standard Recovery Intrusion Detection**	**Awareness SPAM Social Engineering Data Loss / Data Leakage Phishing Security Policy**	**Media Gateways Communication Assisted Law Enforcement (CALEA) Signal Control Points (SCP) Gateway to Gateway Protocol SS7**
Rodney Buie	**Chris Garner**	**John Knies**	**Fred Fletcher**	**Robin Howard**
Micah Maciejewski	Jim Payne	Doug Peck	Ramesh Sepehrrad	Doug Davis
Gary Toretti	Ray Singh	Rajeev Gopal	Allison Growney	Uma Chandrashekhar
Bill Garret	Barry Harp	Ron Mathis	John Coleman	
	Bill Garret	Jeremy Smith		

Methodology (cont.)

Identity Mgmt (6) **Idm Lifecycle** **Access Control** **Strong Authentication** **Certificates** **SAML** **Policy** **Password** **Role Base Access Control** **Systems Administration**	**Martin Dolly** Jim Payne Brian Moir Rajeev Gopal Ray Singh
Encryption (7) **Encryption Keys** **Cellular Networks** **Device Encryption** **Voice Encryption** **Data Encryption** **Key Management** **Key Recovery** **Cloud** **Standards**	**Dan Hurley** Ron Mathis John Rittinghouse Tim Thompson Jim Ransome Anthony Grieco Annie Sokol Bob Thornberry
Vulnerability Mgmt (8) **Alerting** **Risk & Vulnerability Assessment** **Mitigation** **Asset Inventory** **Patch Mgmt**	**Micah Maciejewski** John Knies Jeremy Smith Fernandez Francisco Rodney Buie
Incident Response (9) **Policy & Plan** **Prevention** **Attack Detection** **Response & Mitigation**	**John Rittinghouse** Barry Harp Robin Howard Myrna Soto Fred Fletcher

Findings

- ❑ **Wireless** - Rapid changes in technology continue to evolve in the Wireless space, e.g. 3G to 4G, home cell towers (Femto), smart phones, and wireless “everything”. This is a key focus area that will continue to evolve.
  - ❑ 47 new Best Practices (BPs), while modifying only 3 existing BPs and leaving 2 NRIC VII BPs unchanged

- ❑ **IP Services** - High speed broadband has expanded rapidly to the home and small business. Voice over IP has also grown dramatically as most service providers offer reliable and integrated products with their broadband and IP TV offerings. Additionally, the newest platform service being offered under the title of “Cloud Computing” is quickly redefining the terms “network” and “perimeter”.
  - ❑ 21 new Best Practices in this area, while modifying 7 existing BPs and leaving 2 NRIC VII BPs unchanged

Findings

- ❑ **Network** - The existing NRIC Best Practices are valid and should remain in effect, however with the proliferation of the above mentioned portable devices new best practices have been identified and should become a part of the CSRIC Best Practices documentation.
  - ❑ 23 new Best Practices in this area, while modifying 66 existing BPs and leaving 32 NRIC VII BPs unchanged.

- ❑ **People** – SPAM, Social Engineering, Data Loss / Data Leakage, and Phishing continue to grow; creating havoc among Service Providers, Network Operators, and Government. Security Awareness continues to spread, however, with limited effectiveness. These areas have been, and continue to be critical areas that must be addressed.
  - ❑ 20 new Best Practices in this area, while modifying 9 existing BPs and leaving 7 NRIC VII BPs unchanged.

Findings

- **Legacy** – Best practices specifically documented for the SS7 network access control, authentication, DoS protection, network design, and link diversity need to be modernized. Media Gateways, CALEA, and Signal Control Points existing Best Practices were reviewed and replaced with new Best Practices.
  - 23 new Best Practices in this area, while modifying 66 existing BPs and leaving 32 NRIC VII BPs unchanged.

- **Identity Mgmt** – A critical area across all networks and systems and made more difficult with the spread of key stroke capturing Botnets.   With Cloud Services and the inter-operable environments with vendor partners, Federation of Identities is occurring at a rapid pace, although basic identity management principles still apply.
  - 8 new Best Practices in this area, while modifying 12 existing BPs and leaving 9 NRIC VII BPs unchanged.

Findings

- **Encryption** – Data at rest / data in transit across data and cellular networks requires protection of the PII information. Key Management is critical for validation and authentication .
  - 8 new Best Practices in this area, while modifying 7 existing BPs and leaving 4 NRIC VII BPs unchanged

- **Vulnerability Mgmt** - Vulnerability Management continues to be a very challenging area due to the proliferation of zero-day exploitation of vulnerabilities, extensive malware infections from websites and spam mail and the general availability of Botnet tool kit targeted to "entry-level" hackers from the sophisticated attackers.
  - 9 new Best Practices in this area, while modifying 15 existing BPs and leaving 9 NRIC VII BPs unchanged.

Findings

- ❑ **Incident Response** - All organizations face interruptions to normal business processes. The ability to accurately forecast and budget for outages caused by security breaches continues to be a much desired business tool that has grown in importance as the reliance on information technology systems has grown
  - ❑ 7 new Best Practices in this area, while modifying 35 existing best practices and leaving 7 NRIC VII BPs unchanged

Recommendation

- ❑ CSRIC Working Group 2A recommends the new set of 397 best practices across the 9 focus areas to the FCC for consideration of adopting the best practices for general use by the communication industry.
  - ❑ As threats become increasingly complex and persistent, network providers, operators, and equipment suppliers must work together within increased diligence to secure the network infrastructure.

Future Considerations

- Service Provider Network Protection
  - Trojans, Botnets, viruses, etc. continue to plague many of these devices and re-infecting them and other devices that communicate with the infected hosts. These devices normally connect to the internet via an Internet Service Provider (ISP). Working Group 8 examined this area and made recommendations for Best Practices. Working Group 2A believes this subject needs additional analysis since it is constantly evolving and recommends a new group should be formed with industry subject matter experts in malware detection, and remediation to assess other ideas and recommendations (such as a central clearing house for Blacklisted URLs).

- Border Gateway Protocol
  - BGP's primary function is the exchange of network reachability information between networks (called autonomous systems), to allow each AS on an internetwork to send messages efficiently to every other interconnected network. Most (if not all) public IP space is interconnected with BGP.   It is our recommendation that a new sub-group be formed with industry subject matter experts in BGP and inter-networking to formally address the needs of this vital part of our infrastructure.

Future Considerations

- Service Provider Network Protection
  - Video on Demand allows users to select and watch video or audio content on demand. Working Group 2A recommends future Councils analyze Best Practices in these areas as the mature in the coming years.

Conclusion

The CSRIC Working Group 2A spent more than nine months researching, analyzing, and evaluating Cyber Security Best Practices. During this time members participated in dozens of conference calls, met in various cities, identified gaps, and researched new Best Practices, plus dedicated countless hours editing and revising the final report.

In conclusion, members feel this Final Report is a fair and accurate representation of their collective view-points and perspectives and hopes this will help to improve Cyber Security through these Best Practices.