Testbed for Cellular Telecommunications Cyber Vulnerability Analysis

Brian Van Leeuwen, Vincent Urias, Casey Glatter, and Alex Interrante-Grant
Sandia National Laboratories**
Albuquerque, USA
{bpvanle, veuria, cglatte, aminter}@sandia.gov

Abstract – Cellular networks play an increasing role supporting critical government, including military and private information systems. Enhanced capability and ubiquity of mobile devices (i.e., smartphones) is resulting in increasing cyber exploit developments targeting the smartphone and growing concern of exploits targeting the cellular infrastructure. Telecommunication advances such as Long Term Evolution (LTE) and Internet Protocol (IP) Multimedia Subsystem (IMS) continue to move cellular communications to an all IP core. An all IP core is part of the move to Next Generation Network (NGN). However, the transition to NGN is expected to occur over time, and during the lengthy transition period multiple generations of telecommunication must coexist and interoperate. Legacy telecommunication equipment such as 3G cellular communications and the public switched telephone network (PSTN) must interoperate with modern telecommunication equipment such as 4G/LTE and IMS. Cellular telecommunications provide IP connectivity to external networks including the Internet. Thus, both legacy and NGN cellular telecommunications are vulnerable to the same classes of threats as other networked computer systems connected to the Internet, in addition to threats associated with their legacy systems. Cyber security analysis of these systems remains a significant challenge. Traditional techniques such as red-teaming, vulnerability assessments, and penetration testing are often unsatisfactory and limited in scope because of the lack of access to telecommunication infrastructure equipment. The consequence is that the effects of a cyber-attack on cellular telecommunications are often unknown.

In order to provide greater cellular telecommunications security posture and insight to system providers, equipment manufacturers, and researchers, security analysis of these systems must occur. Performing experiments on telecommunication systems or on a telecommunication testbed is a key part of security analysis. To overcome the problems with security analysis using expensive telecommunication hardware, Sandia National Laboratories has developed a cellular telecommunication cyber-security analysis testbed using physical hardware, extensive virtualization and emulated machines, and simulation to answer complex system questions about cellular systems and their interaction with legacy and NGN fixed systems. In this paper we will discuss the testbed development and components, several use-cases that were executed during the course of the study which leverage the testbed, the types of cyber-attacks that can be assessed, and the class of questions security analysts can now ask and answer about cyber-attacks against cellular systems. In the use-cases we used the testbed to assess the system-level impacts when published component-level vulnerabilities are exploited by a red team.

I. INTRODUCTION

The use of mobile and cellular wireless communication systems is increasing rapidly throughout the world and driving significant change in the supporting technologies. Technology developments are advancing capabilities in both the handset (i.e., user equipment), and the supporting cellular infrastructure. Much of the technology advances are moving cellular systems to Internet Protocol (IP) technology. Cellular systems along with much of the broader telecommunication systems are moving towards full-IP systems. Telecommunications migration to full-IP is seen in technologies such as Long Term Evolution (LTE) and Internet Protocol (IP) Multimedia Subsystem (IMS) [1]. A full-IP core is part of the move to Next Generation Network (NGN). However, the transition to NGN is expected to occur over time and during the lengthy transition period, multiple generations of telecommunication must coexist and interoperate. Legacy telecommunication equipment such as 2G and 3G cellular communications and the public switched telephone network (PSTN) must interoperate with modern telecommunication equipment such as 4G/LTE and IMS. Telecommunication system technologies associated with PSTN connectivity must coexist with packet-based systems such as voice-over-IP (VoIP). In addition, cellular telecommunications provide IP data connectivity to external networks including the Internet.

Cellular telecommunications are a key aspect of global communications and must provide reliable and secure telecommunications to the public. In years past, much of the telecommunication industry security was achieved through having specialized and difficult to obtain networking components, such as legacy PSTN equipment. However, as the telecommunication industry migrates to NGN, much of the network architecture and protocols are considered open with detailed specification easily available. Thus, with its open architecture and IP-based functionality, NGN and cellular technologies bring security challenges. The security challenges include those from legacy-only equipment, but also include security challenges associated with the Internet, such as cyber-attacks, viruses, and malware. In addition, security is further challenged by the coexistence of legacy architectures and equipment with NGN telecommunication architectures and equipment.

Currently, there are reports and publications on various security vulnerabilities associated with telecommunication architectures and systems. The security vulnerabilities range from those associated with mobile handsets, cellular base stations, the wireless link providing connectivity between the handset and cellular base station, other cellular equipment, and infrastructure networks. Mobile handset security vulnerabilities can be associated with smartphone applications that perform malicious actions [2]. In Global System for Mobile (GSM) communication systems a spoofed base station can be used to intercept and re-route outbound calls [3]. A commonly used encryption cipher used to secure the wireless connectivity of a GSM cellular connection can be intercepted and decrypted using a publicly available algorithm to discover the encryption key [4]. Connectivity between cellular equipment and IP infrastructure

** Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

978-0-7695-5124-1/13 $31.00 © 2013 IEEE
DOI 10.1109/MILCOM.2013.236

equipment relies on protocols that, if not secured properly, can be manipulated to perform a range of malicious modifications to the communications. Many publicly available reports exist on descriptions of security vulnerabilities of the Internet and IP-networking technologies and protocols. With the layered-architecture of IP-based networks, attempts are made to overcome security vulnerabilities with employment of additional protocol layers intended to provide added functionality and security. An example is the deployment of the IMS overlay architecture where vulnerabilities are mainly associated with the enabling protocols, [5] [6]. The protocol vulnerabilities should be considered in an overall system-level security analysis to determine the consequences of an IMS attack on the overall communication system.

The cellular communication system providers and technology developers continue to develop NGN solutions that interoperate with legacy communications and recognize the need for cost-effective end-to-end security solutions. The end-to-end security solution must protect against malicious and inadvertent attacks; provide high availability, reliability, integrity, scalability; and provide accurate billing information. As various communication subsystems are combined in an end-to-end system, the system-level architecture will define the security strength. Analysis of the overall end-to-end security must also be available to determine its effectiveness. A key part of system-level security analysis is performing experiments on communication systems or on a communication system testbed.

To overcome the problems with security analysis using expensive telecommunication hardware, Sandia National Laboratories (SNL) has developed a cellular telecommunication cyber-security analysis testbed using physical hardware, extensive virtualization and emulated machines, and simulation to answer complex system questions about cellular systems and its interaction with legacy and NGN fixed systems [18][19]. In this paper we will discuss a testbed developed by SNL to assess system-level security. Additionally, several system-level use-cases are described. The use-cases demonstrate the effectiveness of using the testbed to determine system-level effects of exploited vulnerabilities and thus identify the vulnerabilities that have the largest consequences. The testbed also enables the analysis of vulnerability mitigation approaches.

II. CELLULAR COMMUNICATION END-TO-END SECURITY ANALYSIS

Voice and data communications performed using cellular infrastructure incorporates interoperability among multiple communication domains and information system technologies. The communication domains include the cellular components such as the handsets, wireless connectivity, base station infrastructure, service provider multimedia infrastructure, and necessary LAN and WAN connectivity. In addition, the PBX, a PSTN component, is a communication domain that interfaces to a cellular system and thus can affect end-to-end security. A security compromise in any of the communication domains or information system technologies can render adequate security in another domain ineffective. Therefore, end-to-end security (i.e., system-level security) should be assessed, rather than limiting a security analysis to the individual components or sub-systems. However, the system-level security approach requires and benefits from security analysis of the individual communication domains, subsystems, and technologies.

In order to assess the end-to-end security of the various cellular system communications, we hypothesize attack vectors that are comprised of individual vulnerabilities associated with each of the various subsystems. We use security reference model ITU-T X.805 [7], which is based on a hierarchy of network equipment and functionality groupings. The ITU-T X.805 security layer groupings are the: infrastructure security layer, services security layer, and application security layer. The three layers support three types of activities represented by security planes: management plane, control plane, and user plane. For example, an exploit that disrupts the infrastructure control messaging (i.e., spoofing DNS) can result in a user connection to an application server in a spoofed IMS instantiation. These system-level security vulnerabilities are best assessed in a testbed comprised of the various cellular system communication domains and information system technologies.

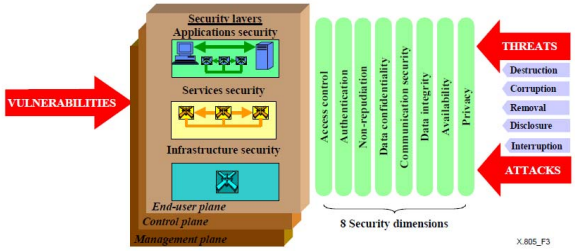

Figure 1: Security architecture for end-to-end network security [7]

Our security analysis approach using a testbed capability requires the various communication domains and information system technologies to be realistically represented. This is achieved using a modeling approach that creates faithful representations of the various communication domains and information system technologies. The realistic representations of the domains and technologies are described in emulation taxonomy. Each domain and technology has realistic representations of its management, control, and user plane data flows and is represented such that a full model can be constructed and used for a security analysis experiment.

III. MODELING APPROACH AND SYSTEM EMULATION TAXONOMY

The vulnerability analysis approach described in this paper is intended to assess the system-level security of cellular communication systems and its interoperability with other communication domains and information system technologies. Our approach employs knowledge of vulnerabilities associated with various subsystems and connecting communication system domains, and assesses their system-level impacts, if exploited, in combination or across multiple similar domains. Our approach identifies the vulnerabilities associated with various subsystems, combines subsystems into a working model, and executes attacks to assess the system-level impacts. STRIDE [8] is a threat model used to categorize the objective of the attacks. The model is applied at system-level and stands for: Spoofing,

Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.

An effective method to perform system-level security analysis is to examine system effects when vulnerabilities are exploited. It is obvious that an analyst would not choose to perform security analysis on an operational system due to the potential of unintended side effects occurring. Testing cyber security tools and evaluating their effectiveness is best performed on non-operational systems that can be returned to a non-corrupted state if an experiment results in a corrupted system. In addition, a key part of telecommunication system security is the human operators that monitor and perform system security operations such as removing live viruses or malware from an operational system. The training and development of processes should not be done on live systems, but on system models that replicate the telecommunication system under study.

The system-level cyber-security analysis capability employs a system modeling approach using emulation, physical hardware, and extensive virtualization. The modeling capability proves effective at incorporating necessary levels of realism for analysis. The system-level modeling includes distributed, replicated subsystems to create experiments of increased scale while maintaining high-levels of realism. The modeling capability includes methods of traffic generation, experiment instrumentation, and data analytics. A system-level model is created by integrating multiple communication domains including the mobile handsets, wireless connectivity, base station infrastructure, service provider multimedia infrastructure, LAN and WAN connectivity, and PBX functionality.

A. Mobile Handset (i.e., User Equipment)

Cellular security has mainly focused on the handsets since they are easily obtained and users have full access to their functionality. SIM cards can be removed and modified. Smartphone handsets can have malicious applications installed. The handsets have received the majority of commercial security solutions. The methods to emulate a handset include incorporating a real handset in the experiment, and using a highly abstracted terminal connected via wired communication link to the infrastructure.

In stand-alone security experimentation involving the wireless link, a real or surrogate handset with an actual wireless transceiver is necessary. For example, experiments addressing the plausibility of causing a handset to migrate from one GSM base station to another base station require full wireless connectivity. These experiments also assess the level of difficulty to force a handset to connect to a spoofed base station and to assess technologies that prevent this malicious behavior.

Numerous other security analysis and experiments are performed where the wireless link connectivity is abstracted away. In these experiments, the handset functionality does not require the wireless link connectivity components and thus more abstracted handset emulators are used. The selection of handset emulator types is dependent upon the class of security analysis being performed. In some cases, a terminal that provides short message service (SMS) texting is used to assess security of the infrastructure that forwards and manages SMS texting. In other cases, a more sophisticated handset emulator is used to emulate a smartphone running Android OS and specific applications. Another handset emulator creates the necessary smartphone connectivity used to engage the IMS infrastructure. Experiments performed at increasing scale employ the emulated handsets and can be increased significantly above the experiment using actual wireless links.

B. Wireless Connectivity Infrastructure

A major challenge of assessing systems that include wireless connectivity, such as that from a GSM handset to a GSM base station, is the isolation requirement of the wireless emissions. In the case of GSM cellular communications, the wireless connectivity occurs in licensed spectrum, therefore any uncontrolled emissions can violate spectrum ownership. However, the security analysis of the wireless connectivity is important to assess the plausibility of an intruder to exploit weaknesses in wireless channel security. Furthermore, security analysis involving handset connectivity to base stations is best performed with a fully connected handset that must utilize the full connection protocols with the base station. For experiments that require complete wireless connectivity, our methodology employs the necessary RF isolation by using RF shield boxes [9].

Our methodology includes a stand-alone experiment platform capability that is used to perform small-scale analysis involving wireless telecommunication equipment. In order to achieve realism in wireless link connectivity, it is necessary to deploy actual hardware that incorporates the required radio transceivers and link protocols. In our experiments this includes actual mobile handsets that are equipped with the necessary credentials to access the associated infrastructure base station. In the case of GSM and its packetized data link capability, General Packet Radio Service (GPRS), a hardware base station can be obtained and configured to create an operational cellular wireless link. The wireless connectivity faithfully represents an actual GSM/GPRS to base station link. In addition, security exploits that enable eavesdropping of the wireless channel have been identified. In order to assess the capability and mitigation of eavesdropping software, it is essential to create a realistic experiment that can produce an actual encrypted wireless link. Once an operational wireless link is created, a means to passively capture the GSM/GPRS wireless connectivity for post processing is necessary. In our experiments, a highly-configurable software defined radio (SDR) is configured and deployed to passively capture the encrypted data-streams transported over the link [10]. In this experiment the handset, base transceiver station, and SDR are all deployed in the RF shielded box.

Experiments that include actual wireless transmissions are performed on a small-scale because of limitations controlling increased-scale wireless emissions. Furthermore, larger-scale experiments of this kind require increased numbers of base station equipment that must be deployed. This can be costly and time consuming.

C. GSM Base Station Controller

For the stand alone experiments that include a packet-data capable smartphone handset and base station transmitter, emulation of GSM infrastructure components called GPRS support nodes are also required. The two GPRS support nodes are:

- Serving GPRS support node (SGSN): Enables authentication of GPRS mobiles, registration of mobiles in the network, mobility management, and collecting information on charging for the use of the air interface.
- Gateway GPRS support node (GGSN): Provides routing to external networks and tunnels packets through the IP-based internal backbone to the correct Serving GPRS Support Node.

With this infrastructure, emulated packets created at the handset can be transmitted through the infrastructure components and into larger IP-based networks. Security analysis requiring this connectivity can be performed and protocol interactions between the entities can be instrumented and monitored for security analysis purposes.

D. IP Multimedia Subsystem (IMS)

IP Multimedia Subsystem (IMS) is an architectural framework for delivering IP multimedia services and enables fixed-mobile convergence. The IMS architecture consists of session control, connection control, and an application service framework that enables the access of multimedia (e.g., voice, video, chat) from wireless and wired terminals. As an example, with IMS one can start with chat, add voice (for instance Mobile VoIP), add another caller, add video, share media and transfer files, and drop any of these without losing or having to terminate the session.

IMS is a key enabler of NGN and mainly utilizes IP protocols such as Session Initiation Protocol (SIP), to establish sessions across wired and wireless networks; Session Description Protocol (SDP), for media negotiation; and Real-time Transport Protocol (RTP), for media transmission. A primary function of IMS is authentication, authorization, and accounting (AAA) that is performed in coordination with the Home Subscriber Server (HSS) using the Diameter protocol [11]. IMS is comprised of several main components: Proxy Call Session Control Function (P-CSCF), Interrogating-CSCF (I-CSCF), Serving-CSCF (S-CSCF), Media Gateway Control Function (MGCF), Media Gateway (MGW), and HSS. The various CSCFs are SIP-based servers. A high-level view of the IMS architecture is shown in Figure 2 [6].

As cellular communication service providers transition to NGN architectures and deploy IMS architectures, the need for inter-IMS operability between service providers increases. IMS functionality includes mechanisms for interoperability between multiple IMS instantiations. The connectivity is enabled by an underlying supporting IP network infrastructure comprised of local area network (LAN) and wide area network (WAN) components. Security vulnerability analysis should be performed for the various interactions between multiple IMS instantiations. Our cyber security analysis includes a capability to model various networked communication system architectures and underlying network connectivity at increasing scale. In the case of multiple IMS instantiations connected via a WAN, our analysis approach employs extensive virtualization to create multiple IMS instantiations connected by a fully routed WAN infrastructure with WAN emulation. Also represented in the cyber experiments are key network infrastructure services such as Domain Name System (DNS).

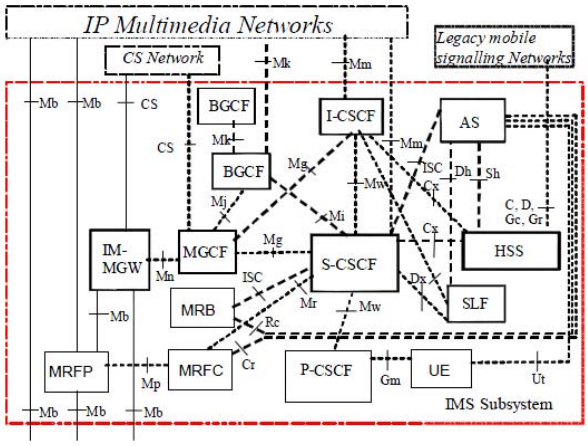

Figure 2: IP Multimedia System (IMS) Architecture [6]

E. LAN and WAN Connectivity

The migration to NGN results in cellular telecommunication employing more IP connectivity. The result is that security issues associated with IP connectivity over LANs and WANs also impact cellular communications. Potential vulnerabilities may exist in the various routing protocols, security devices, and network services that support LAN and WAN connectivity such as BGP routing, firewall implementations, and DNS.

With the cyber security analysis testbed complex network, connectivity can be constructed to provide connectivity between the cellular system and intended data or voice connection. LAN and WAN network vulnerabilities can be exploited to identify the impacts to the cellular system connection. In addition, vulnerability mitigation approaches can be implemented and assessed for effectiveness in eliminating the undesired impact to the cellular connection.

F. Private Branch Exchange (PBX)

A private branch exchange (PBX) is a private telephone network, used within businesses or other organizations, that connects multiple telephone lines to the external PSTN via trunk lines. Current PBX capabilities include technologies that can provide connectivity to VoIP gateways, support conference servers, and provide connectivity to the outside world via the PSTN.

As telecommunication systems evolve into NGN architectures, there is an extended period of time where NGN technologies must coexist and interoperate with legacy technologies. In the case of securing telecommunication systems, the interoperability

between systems at various levels of technology evolution creates potential security vulnerabilities. An example of this required capability is a cellular based VoIP call, communicating through IMS architecture to a PSTN landline telephone using a PBX.

In order to assess the security posture of the broader end-to-end communications that includes a cellular sub-system on one end and a fixed-line PBX sub-system on the other end, an expanded experimentation platform is required. In our security analysis platform we incorporate the Asterisk PBX to provide connectivity to PSTN sub-networks and VoIP calls [12] [13]. Furthermore, our objective to enable security analysis of larger telecommunication network topologies of disparate technologies requires a capability to deploy large networks of telephones.

Tools were developed to achieve the objective of deploying large networks of phones using extensive platform virtualization. A method to automate the deployment of cloud-based servers and softphones (software phones) to represent the PBX infrastructure was developed, leveraging open-source applications such as Distributed Universal Number Discovery (DUNDi) [14]. In addition, as larger network topologies are created for analysis, techniques to create and analyze traffic are necessary, therefore our experimentation platform includes a traffic generation capability using open-source traffic generator SIPp [15] for SIP protocol based traffic.

IV. Cellular Communications Cyber Threats

With GSM or 2G cellular communication systems, the wireless communication channel can be accessed using commercially available equipment and open-source software [3]. In this attack, data can be recorded from the wireless transmission using a Software Defined Radio (SDR). After using GnuRadio tools to record data from the wireless link, the open-source software Kraken [4] can be used to decode the encryption key used to encode the wireless link. The Kraken tools use Rainbow Tables to perform the decoding of the encryption key and thus can be used to decode the voice traffic.

First and second generation cellular communication systems were strictly connection oriented systems that employed control signaling based on the closed SS7 signaling used by traditional telephony systems. The vulnerabilities of the early generation cellular systems were limited and well assessed and thus the threats to these early systems were limited. However, the advent of packet data services and support of IP connectivity not only increased the functionality of the cellular system, but also increased the security vulnerabilities. The cellular systems supported data connectivity that interfaced to the telecommunication IP infrastructure, enabled by either IP-PBXs or IP Multimedia Subsystems (IMS). A primary supporting protocol enabling the interoperability of the cellular system with the infrastructure components is the Session Initiation Protocol (SIP). SIP itself is not inherently vulnerable, as the intention of the protocol is to manage connection sessions from within a secure environment [13]. However, if an attacker gains access to the unsecure data stream, SIP provides a variety of ways to disrupt, hijack, redirect, or otherwise exploit a phone call or IMS registration. Figure 3 illustrates several locations where SIP messages can potentially be accessed and modified.

IMS employs the Diameter protocol for Authorization, Authentication, and Accounting (AAA). Diameter performs the signaling functionality formerly provided by SS7 or RADIUS. Within the IMS control and service planes, Diameter plays a central role in policy, charging, authentication, and mobility management. The Diameter specification allows either IPsec protection or TLS protection to be used to protect its messages [11]. At a system level, an attacker can perform extensive exploits by accessing this protocol via intra-domain channels as shown in Figure 3.

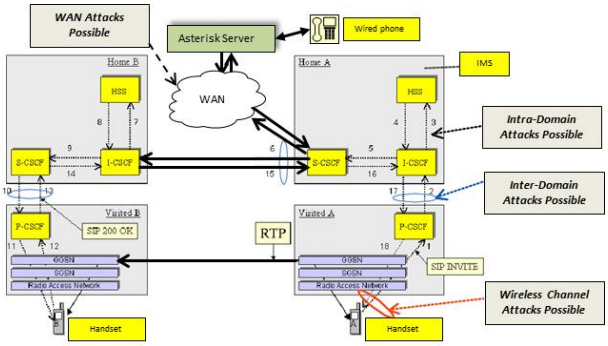

Figure 3: Potential vulnerability locations

As described in previous sections of this paper, the various subsystems of the cellular telecommunication system have vulnerabilities and, in cases, attacks have been identified and published. The attack descriptions are specifically targeted against the subsystems under study and the description of the consequences is limited to those consequences associated with the subsystem.

V. Telecommunication Security Assessment Demonstration Experiment and Setup

Given our hypothesis that system-level impacts are largely untested and not well understood with regard to end-to-end security of the diverse, tightly coupled voice and data communication systems that span multiple communication domains, we created several demonstration use-cases. Our objective was to demonstrate the effectiveness of the testbed and its ability to help answer system-level cyber security questions; and provide an analyst a platform to assess the interactions between the multiple subsystems.

In our demonstrations we explored the interoperability of the various communication domain components, surrogate systems and the integration to faithfully explore end-to-end calls and interactions with the IMS infrastructure. An initial use-case was to place calls across multiple domains. In this use-case we explored how to compose and represent the complexity of a telecommunications infrastructure given both physical and emulated devices. We focused on getting functional calls and interactions between physical devices (such as real cell phones, physical SIP phones) and emulated devices (emulated SIP

clients, emulate cellphones) over both physical (e.g., nanoBTS) and emulated infrastructure.

These experiments demonstrated that that call interactions are faithful per documented standards and connection diagrams. In addition, we conducted experiments to identify the data sources that can be used to assess the security posture of the system. Data sources analyzed included:

- Application logs (Asterisk, OpenIMS),
- Netflow logs,
- nanoBTS logs,
- Handset logs.

Another primary data source used for detecting and assessing system security posture was Wireshark, an open-source packet capture and analyzer application. Wireshark has advanced features including call flow diagrams and expert analysis modes that can help reveal anomalous system behavior. Connection resets, retransmissions, and malformed packets can help reveal the presence of an attack on the system. These data sources were logged to a common platform for analysis. This data is logged and correlated with the events resulting from exploiting various published vulnerabilities.

An additional objective of this research was to develop analytics and security techniques that can provide an indication if the cellular communication infrastructure is under cyber-attack. We focused on several classes of broad threats to the cellular communications infrastructure. First, in an effort to evaluate the fidelity and determine what class of questions/analysis can be conducted on the testbed, we developed a series of evaluations that included inducing failures and exploiting published vulnerabilities. The conducted experiments are based on a variety of cellular system communication scenarios, mostly focusing on evaluating the efficacy of the experimental system, and evaluating if the testbed can faithfully respond to a variety of stimulus and operating conditions. Our objective was to identify and/or develop detection methodologies that can be employed to detect these multi-domain threats.

With the objective of identifying system data sources and analytics to indicate if a system is under cyber-attack, we used red team methods to induce failures and instantiate published vulnerabilities on the testbed. The red-team's attempts at emulating unauthorized accesses were primarily focused on:

- Attempts to achieve unauthorized access to one of the security dimensions noted in Figure 1 by compounding multiple subsystem or communication domains.
- Emulate unauthorized access of single domain published vulnerability. In cases, unauthorized access is not obtained since a security layer in another domain would prevent the unauthorized access.
- Multiple subsystems interoperating as a single cellular system required instantiation of multiple simultaneous vulnerabilities across the multiple subsystems.

Modify/Intercept Phone Calls:
Several system experiments demonstrate the cellular cyber vulnerability analysis methodology and testbed. A small-scale test environment provides single IMS core instantiations along with physical hardware supporting GSM wireless communications. Many articles have discussed and published tools that indicate that GSM cellular systems are vulnerable to a base station being spoofed, intercepted, and man-in-the-middle [21]. In GSM the handset must authenticate to the GSM base station, but the base station is not required to authenticate to the handset. Thus, a malicious GSM base station can be deployed and, if it offers the best connection for a handset, the handset will attach to the rogue base station.

In this small-scale testbed, a controlled Base Transceiver Station (BTS) acts as a rogue component, with multiple smartphones associating and connecting to the malicious BTS. Given this point of presence, there are limited options on what can be done. Given access to the wireless link between the cellular phones and base station, an encrypted call is sniffed using a Software Defined Radio (SDR), decrypted using a public algorithm, and replayed as a normal Real-time Transport Protocol (RTP) stream. Given the data sources that we provided and used, this class of vulnerability could not be easily detected. However, operational systems may use past connection data, characteristic connection volumes for a particular base station, to detect potential rogue BTS components. An abnormal drop in cell phone associations to a base station could be a sign of a nearby malicious BTS.

In 3G cellular systems that include GPRS capability, any data connectivity using an IMS based application will not function if the malicious GSM/GPRS base station does not have connectivity to an authentic IMS. In the cellular vulnerability testbed we are able to create an experiment that includes both a rogue GSM/GPRS base station and a rogue IMS core with necessary registered user agents. This demonstrates that at the system-level, multiple vulnerabilities must be exploited in two interoperating subsystems to compromise the data stream.

WAN Vulnerability Impacts on IMS:
The WAN has numerous known open-source vulnerabilities including DNS spoofing, DNS redirection, DNS man-in-the-middle, ARP spoofing, and BGP redirection vulnerabilities that have been well-documented in numerous venues [17][20]. In cellular communications involving multiple service providers, multiple IMS's are employed for the end-to-end connection. The IMS infrastructure communicates over a WAN infrastructure and we hypothesized that it would be susceptible to the same vulnerabilities as would any IP-enable application. Using the testbed, experiments demonstrated that in a multi-IMS scenario, inter-IMS communication can be compromised in multiple ways. Log data is collected and will be assessed. Since these tests are focused on system-level assessments of the wired infrastructure, the wireless link and physical handsets are abstracted away. This also allows for larger-scale implementations using cloud-based virtual machines and system emulation. The first IMS represents a valid user's home IMS, the second IMS represents the intended recipient of the originating call, and a third represents a rogue IMS. Using Wireshark, anomalies in typical data flows between the multiple IMS's can be detected. System-level knowledge and advanced Wireshark

features such as deep packet inspection and protocol statistics enabled the viewing of abnormal packet exchanges. For example, in the above experiment, a malicious user could use a known DNS spoofing vulnerability to impersonate the network DNS responses and redirect outgoing SIP calls to a rogue IMS. In this case, reviewing the Wireshark SIP statistics would reveal anomalous SIP "INVITE" requests, revealing the presence of an attack. We showed that given WAN vulnerabilities, a malicious user could gain access to unintended information; however, with robust logging and cross-federated log aggregation we are able to detect this class of threats fairly easily.

VI. CONCLUSION AND FURTHER STUDY

Our primary research goal was achieved; we demonstrated real, feasible attacks on a testbed that realistically represented a telecommunications infrastructure consisting of multiple subsystems. The subsystems included 2G cellular with GPRS packet data capability, supporting GSM/GPRS base station connectivity, and multiple IMS infrastructures for application server connectivity. Our testbed successfully integrated realistic telecommunication system protocols and demonstrated some of their weaknesses in an unsecure environment. The primary weaknesses do not necessarily lie within the individual components, but in the overall system-level design. End-to-end trust for IMS cores is assumed, even when the connections must traverse 3rd party components (DNS, WAN equipment, etc.).

System-level security vulnerabilities can be difficult to detect. However, using a combination of advanced networking tools and logging analysis techniques, attack characteristics can be revealed. Experimental testbeds capable of faithfully representing the system-level interactions and communications are essential for these analysis methods to progress and be refined.

In this research, we have developed an important and capable cyber security analysis and experiment environment (i.e., testbed) to help perform analysis of communication networks and networked information systems. With the advent and move towards all-IP networks and NGN, these types of experiments are essential to understanding the securities and insecurities of future cellular telecommunications systems.

REFERENCES

[1] Oredope, A.; Pham, V.; Evans, B., "Deploying IP Multimedia Subsystem (IMS) services in future mobile networks," Communications (NCC), 2011 National Conference on , vol., no., pp.1,5, 28-30 Jan. 2011

[2] Yajin Zhou; Xuxian Jiang, "Dissecting Android Malware: Characterization and Evolution," Security and Privacy (SP), 2012 IEEE Symposium on , vol., no., pp.95,109, 20-23 May 2012

[3] Yubo Song; Kan Zhou; Xi Chen, "Fake BTS Attacks of GSM System on Software Radio Platform," JOURNAL OF NETWORKS, VOL. 7, NO. 2, FEBRUARY 2012

[4] McMillan, R., "New 'Kraken' GSM-cracking software is released - GSM eavesdropping for the masses comes to Black Hat," PCWorld Business Centre, July 22, 2010

[5] Kai Shuang, Siyuan Wang, Bo Zhang, Sen Su, "IMS Security Analysis using Multi-attribute Model," JOURNAL OF NETWORKS, VOL. 6, NO. 2, FEBRUARY 2011

[6] Dong Wang, Chen Liu, "Model-based Vulnerability Analysis of IMS Network," JOURNAL OF NETWORKS, VOL. 4, NO. 4, JUNE 2009

[7] INTERNATIONAL TELECOMMUNICATION UNION (ITU), "X.805: Security architecture for systems providing end-to-end communications," October 2003

[8] Shawn Hernan, et. al., "Uncover Security Design Flaws Using The STRIDE Approach," MSDN Magazine, November 2006

[9] Ramsey Electronics, Inc., Victor, NY, http://www.ramseytest.com/

[10] Ettus Research, Mountain View, CA, https://www.ettus.com/product

[11] Abhayawardhana, V.S.; Babbage, R., "A Traffic Model for the IP Multimedia Subsystem (IMS)," Vehicular Technology Conference, 2007. VTC2007-Spring. IEEE 65th , vol., no., pp.783,787, 22-25 April 2007

[12] Digium Inc., Asterisk, http://www.asterisk.org/

[13] Shawn McGann, Douglas Sicker, "An Analysis of Security Threats and Tools in SIP-Based VoIP Systems," Second VoIP security workshop, 2005

[14] Distributed Universal Number Discovery (DUNDi), http://www.dundi.com/

[15] SIPp, http://sipp.sourceforge.net/

[16] K. Boman, "Network Domain Security (TS33.210) & IMS Security (TS33.203)," Ericsson Brief, February 2003

[17] Avi Kak, "Lecture 17: DNS and the DNS Cache Poisoning Attack," Purdue University, March 2013

[18] Van Leeuwen, B.; Urias, V.; Eldridge, J.; Villamarin, C.; Olsberg, R., "Performing cyber security analysis using a live, virtual, and constructive (LVC) testbed," MILITARY COMMUNICATIONS CONFERENCE, 2010 - MILCOM 2010 , vol., no., pp.1806,1811, Oct. 31 2010-Nov. 3 2010

[19] Urias, V.; Van Leeuwen, B.; Richardson, B., "Supervisory Command and Data Acquisition (SCADA) system cyber security analysis using a live, virtual, and constructive (LVC) testbed," MILITARY COMMUNICATIONS CONFERENCE, 2012 - MILCOM 2012 , vol., no., pp.1,8, Oct. 29 2012-Nov. 1 2012

[20] B. Van Leeuwen, U. Onunkwo, M. McDonald, "BGP analysis using System-in-the-Loop (SITL) testbed," 2008 OPNETWORKS Conference, August 2008.

[21] Website, Cellular Interception: Hacker Developments; http://www.cellcrypt.com/gsm-cracking