

Improving Mobile Core Network Security with Honeynets

Despite improved security, core network vulnerabilities continue to threaten third-generation (3G) mobile systems. This article offers a security assessment conducted in the packet-switched domain of a mobile operator's infrastructure. A honeynet architecture could help address 3G security.



CHRISTOS K. DIMITRIADIS
University of Piraeus

Third-generation (3G) mobile systems provide enhanced security by deploying a mobile terminal to Universal Mobile Telecommunications System (UMTS) Terrestrial Radio Access Network (UTRAN) mutual authentication and by addressing the vulnerabilities in 2G's underlying cryptographic technology.¹ Such systems also pay special attention to user privacy by deploying an identity management scheme to protect the confidentiality of user identity, position, and service delivery.²

With these features in mind, 3G mobile subscribers might feel more secure when connecting to 3G networks, but this perception doesn't reflect reality when you consider all the elements in the service provision path, including the core network. The 3G core network consists of the circuit-switched (CS) domain, the packet-switched (PS) domain, and the Internet Protocol (IP) multimedia subsystem (IMS).³ The CS domain handles traffic switching and signaling for voice communications, linking the UTRAN with other voice networks. The PS domain handles traffic switching and signaling for data communications, linking the UTRAN with other packet domain networks (PDNs) such as the Internet; the IMS is a complementary subsystem that provides multimedia services over the PS domain. This article focuses on the open security issues in the PS domain—in particular, how honeynet technology can be a cost-effective solution that increases security.

Core network security

In recent years, mobile telecommunication networks have transformed from infrastructures that provided

voice and limited data services to infrastructures that offer a wide range of multimedia options.⁴ The new demands on service provisions require improved versions of supporting systems for charging and billing, roaming, and addressing, as well as the necessary security services for protecting the confidentiality, integrity, and availability of all types of information, including user traffic, signaling, and control data.⁵

The outcome of this transformation was an upgrade from the existing closed Signaling System 7-based networks to IP-based systems that combine several old and new technologies and applications under the pressure of timely service delivery startup. Several research studies report the security vulnerabilities that have subsequently arisen:⁶⁻¹⁰

- a lack of intrusion detection systems (IDSs);
- inadequate firewall architectures;
- no security layers; and
- uncontrolled communication with roaming partners.

Such vulnerabilities ultimately lead to threats, which fall into these categories:

- billing attacks via gateway filters;
- exposure of critical production systems that implement packet switching—such as gateway general packet radio service (GPRS) support nodes (GGSNs) and serving GPRS support nodes (SGSNs)—to attacks;
- exposed GPRS elements used as springboards for critical system attacks, such as the home location register (HLR), which is the main database of permanent sub-

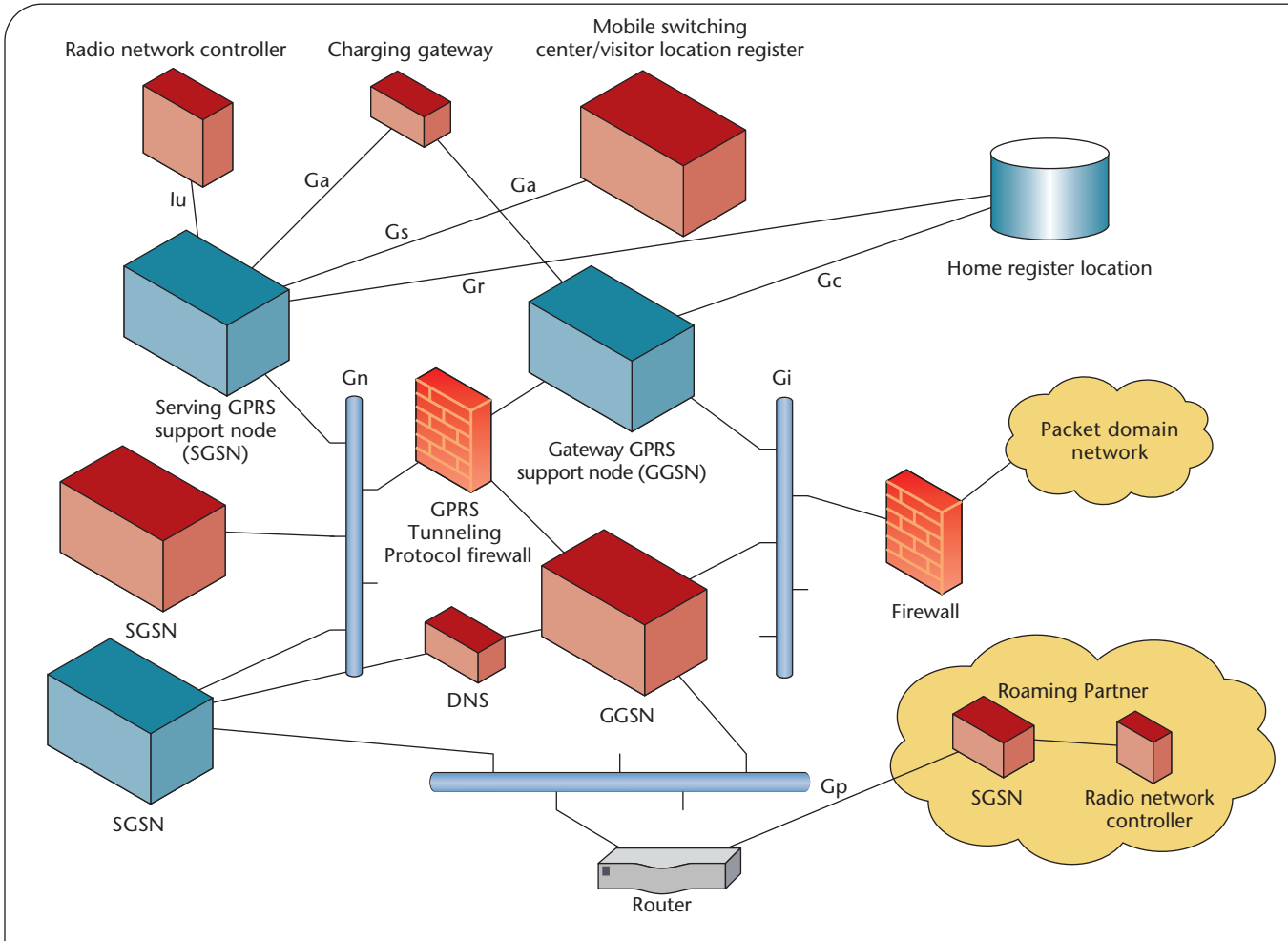


Figure 1. System overview. A compromised serving general packet radio service (GPRS) support node (SGSN) or gateway GPRS support node (GGSN) affect many different systems (in red). (Ga, Ge, Gi, Gn, Gp, and Gr are the various interfaces.)

scriber information, the mobile switching center (MSC), which implements voice circuit switching, the charging gateways (CGs), or the billing gateways (BGs); and

- the mobile operator’s core network turned into an extension of a roaming partner’s core network, exposing both to serious attacks.

Figure 1 gives an overview of the systems in a 3G network affected by a compromised SGSN or GGSN, due to inadequate security architectures.

In fact, a compromised SGSN or GGSN exposes several systems to attack, including the network’s other SGSNs and GGSNs; the HLR; the MSC or visitor location register (VLR); the CG; the radio network controllers (RNCs), which control the base stations (and implement radio resource and mobility management); the DNS, any roaming partners’ infrastructures; and other PDNs. The firewall in the Gi interface, which is the interface between GGSNs and external PDNs, is a com-

Glossary

AG	attack group
BG	billing gateway
CG	charging gateway
CS	circuit switched
IMS	IP multimedia subsystem
GGSN	gateway GPRS support node
GPRS	general packet radio service
GTP	GPRS Tunneling Protocol
HLR	home location register
MSC	mobile switching center
PS	packet switched
PDN	packet domain networks
PDP	Packet Data Protocol
RNC	radio network controller
SGSN	serving GPRS support node
VLR	visitor location register

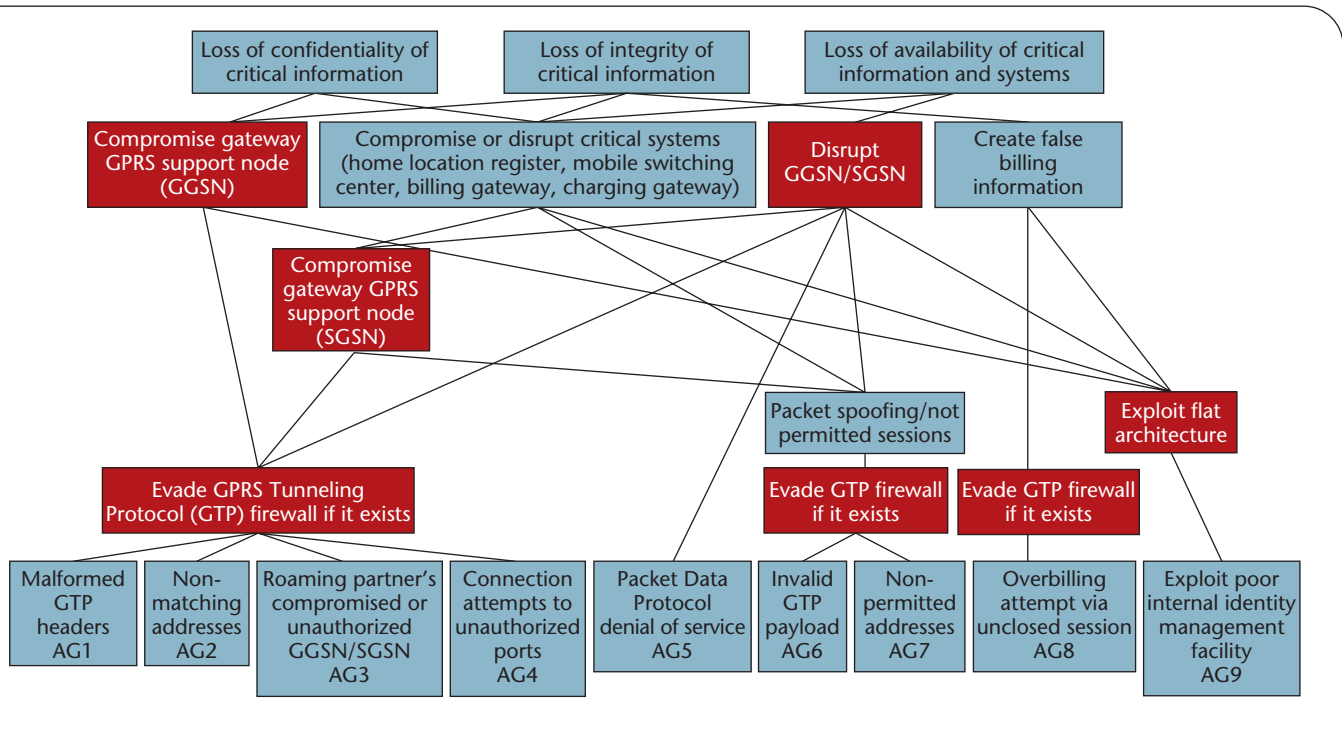


Figure 2. Combined attack trees. The leaf nodes in red highlight where the proposed solution blocks each attack path.

mon countermeasure for filtering communication. Communication between SGSNs and GGSNs occurs via the GPRS Tunneling Protocol (GTP) over the Gn interface, which is the interface between the SGSN and GGSN. GTP-aware firewalls usually control this interface when IDSs aren't present. The Gp interface, which is the interface between a mobile operator's SGSN and GGSN and a roaming partner's corresponding systems, is likewise inadequately controlled: security is limited by the implementation of typical packet filtering in the BG.

The security assessment described in this article also revealed that legacy systems (such as those used for billing) don't provide adequate facilities for logging user actions. This insufficient logging facility in combination with nonexistent IDSs affects the timely identification of an intrusion, as well as post-attack forensics. Moreover, the study identified inadequate identity management mechanisms in the PS domain, including in shared accounts for accessing critical systems.

Threat model

Within the scope of an assessment, we must create a threat model to correlate these identified vulnerabilities with the corresponding threats and business impacts, as well as the attack steps for exploiting the vulnerabilities. A threat model describes the threats that attackers can realize by exploiting vulnerabilities. We can depict it graphically by using a combination of attack trees,¹¹ each of which has a root node, leaf nodes, and child nodes. The root node represents the attack

target, the leaf nodes represent the means for reaching the target, and the child nodes represent the events that comprise the attack. All leaf and child nodes have an OR logic. Figure 2 shows a combination of attack trees.

The combined attack trees in the figure have three root nodes, one for each final target. Taking into account that the overall target is a security breach, the three root nodes correspond to a breach of each of the system's security cornerstones: confidentiality, integrity, and availability. To reach a target, an intruder might use one of the leaf nodes, which are the compromised or disrupted critical systems (including the GGSN and SGSN), or create false billing information.

Various attack groups (AGs) explain each path of the attack trees. In AG1, GTP packets with malformed headers might lead to GGSN or SGSN compromise or disruption (such attacks exploit badly configured or nonexistent GTP firewalls). In turn, the compromised GGSN or SGSN can become a springboard for attacks on other critical systems by exploiting the mobile operator's flat architecture, with its lack of security zones. In any case, a critical system's compromise can lead to a loss of data confidentiality or integrity, while service disruption can lead to a loss of availability (via denial of service). Other attacks also exploit badly configured or nonexistent GTP firewalls, often with the same results:

- AG2 is the submission of non-matching addresses between the GTP payload (encapsulated packet) and the

assigned address as defined in the Packet Data Protocol (PDP) context handshake.

- AG3 is a connection attempt from a roaming partner's unauthorized or compromised SGSNs or GGSNs; it exploits the poorly controlled communication path connecting two networks.
- AG4 is an attempt to connect to target systems in administration ports (generally, any attempt to connect to a port other than the standard GTP ports).
- AG5 is an attempt to initiate a great many PDP contexts, which could result in the disruption of a GGSN or SGSN, leading to loss of system availability.
- AG6 is a GTP packet with an invalid payload, which could result in packet spoofing and non-permitted sessions.
- AG7 is a GTP packet with a payload that contains non-permitted source or destination addresses, which can result in packet spoofing and non-permitted sessions.
- AG8 is an over-billing attack based on open sessions in which a specific IP address requests data from a server and releases the IP address, which is then reassigned to a new user. The new user keeps receiving the data and thus gets over-billed.
- AG9 is the exploitation of non-network-based vulnerabilities, such as poor identity management facilities. This AG focuses on insider attacks caused by uncontrolled communication between critical systems.

Both to identify the severity of successfully implementing the attacks described here and to complete the threat model, we must define the business impact. Successful attacks have several business impacts:

- *Direct and indirect monetary loss* could be the result of denial of service or lost charging and billing data.
- *Loss of reputation* could be a side effect of exposing confidential subscriber data or damaging a roaming partner via a security incident initiated from an SGSN or GGSN.
- *Legal problems* could result from exposed confidential subscriber data or being unable to address contractual obligations with third parties.

The knowledge and skills for launching a successful attack against a mobile operator's core network varies, depending on the operator's security architecture. At a minimum, the attacker needs basic knowledge about the target system's operation and vulnerabilities. However, the possibility for realizing an attack increases due to the sensitivity of the information handled in a 3G infrastructure—for example, the disclosure of subscriber call details is a strong motive for adversaries who want to invade subscribers' privacy or impact a mobile operator's overall business infrastructure.

Honeynets in 3G: Feasibility study

A honeynet is an information systems architecture whose value lies in its unauthorized or illicit use, which helps security engineers learn from attacking entities and thus improve existing security architectures and systems.¹² The honeynet's heart is a gateway called a honeywall, which controls and captures network packets both to study them and to protect other information systems from attacks launched from potentially compromised systems inside the honeynet.

The honeynet proposed in this article—3GHNET—offers a way to improve 3G core network security because it's

- *Preventive.* As a decoy, it's an easy target for attackers and distracts them from the mobile operator's production systems.
- *Detective.* It helps identify and analyze potential attacks against production systems.
- *Reactive.* Detection of an attack not only warns and prepares security engineers for a possible attack against a production system but also gives them valuable knowledge for fixing the existing security architecture.

To study the benefits of implementing 3GHNET, we used concepts from game theory, which is a set of applied mathematical models that aim to study cooperative and conflicting interactions with formalized incentive structures.¹³ Its foundations lie in Augustin Cournot's "Researches into the Mathematical Principles of the Theory of Wealth."¹⁴ Game theory was founded as a scientific field by John von Neumann in 1944, with his publication of "The Theory of Games and Economic Behavior," which he wrote in collaboration with Oskar Morgenstern.¹⁵ In 1950, John Nash introduced a related principle called Nash equilibrium, proving that the best responses of all players are in accordance with each other.¹⁶

We wanted to compare a mobile operator that implements a honeynet with one that doesn't, and then study different security situations. For this purpose, we defined a game called 3GHNET-G that is non-cooperative—the mobile operators don't have a common security infrastructure, and the game is static because players can make simultaneous moves. 3GHNET-G is also a non-zero sum game, meaning that the total benefit to all players isn't zero because there's no relationship between one player's gain and another's loss.

3GHNET-G has a set of players (N), a set of strategies Σ , and a set of payoffs P , defined by the following expression:

$$\pi : \prod_{i \in N} \Sigma^i \rightarrow P$$

Table 1. Gain types and values.

GAIN ID	DESCRIPTION	GAIN VALUE
G_1	Self-security from internal nodes	10
G_2	Security from external nodes	10
G_3	Security to external nodes	10
G_4	Knowledge	10
G_5	Cost	-5

Table 2. Payoff matrix of 3GHNET-G.*

	ATTACK (MO2)	NORMAL (MO2)
Attack (MO1)	35, 10	25, 10
Normal (MO1)	15, 10	-5, 0

*Bold denotes the Nash equilibriums, the conditions that give both players a mutual best advantage.

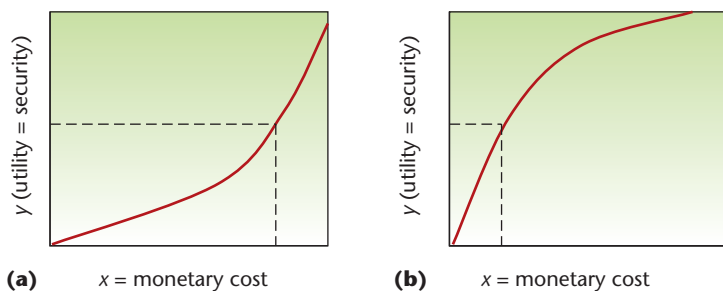


Figure 3. Risk-averse vs. risk-seeking behavior. The curve on the left shows an entity that is willing to invest more money in security, whereas the opposite is true on the right.

where $N = \{1, 2\}$, Σ^i is the strategy space of player i , and $P \rightarrow R^N$ is the players' payoff at the end of the game.

For our two players, mobile operator 1 (MO1) implements a honeynet architecture, and mobile operator 2 (MO2) doesn't. Each player has two possible strategies—or more precisely for our study—modes of behavior, depending on whether a security incident compromises the player's nodes or not:

- $\Sigma 1$ represents compromised node behavior, and
- $\Sigma 2$ represents normal node behavior.

As with N earlier, $\Sigma^i = \{\Sigma 1, \Sigma 2\}$. By following this logic and not studying the gain from possible player moves, we study the gain of implementing a honeynet or not in different security-related situations.

The payoff gets specific values from a definite set $P =$

$\{P_1, P_2, \dots, P_m\}$. Let each possible payoff P_i (where $i = \{1, 2, \dots, m\}$) be a sum of gains from Table 1, depending on a specific condition.

The first three gains correspond to the threats described in the previous section, including insider attacks and those to and from external nodes (especially roaming partners). The fourth gain corresponds to the knowledge produced by a security architecture that can study attacks and evolve in response to attacker tactics. The last gain is negative, corresponding to the cost of implementing the honeynet.

We define the payoff P_i through the following equation: $P_i = a_1 G_1 + a_2 G_2 + a_3 G_3 + a_4 G_4 + a_5 G_5$. The parameters $a_n = \{0, 1\}$, where $n = \{1, 2, 3, 4, 5\}$, take a positive value when the player receives the corresponding gain in a specific condition and zero value in the opposite scenario.

A game's payoff matrix shows what payoff each player will receive at the game's outcome; it depends on the combined actions of all players. Table 2 shows 3GHNET-G's payoff matrix.

When both operators experience compromised nodes, we have an attack-attack condition: MO1 receives all the gains in Table 1, which include protecting its internal nodes, preventing attacks on other mobile operators, gaining knowledge, and paying the honeynet cost. MO2 (the player without the honeynet) only receives gain G_2 because it's protected from MO1's compromised node by the honeynet. In an attack-normal condition, MO1 doesn't receive the G_2 gain because MO2 isn't attacking, but it receives the rest of the gains as in the previous condition; just as in the previous condition, MO2 receives gain G_2 . In a normal-attack condition, MO1 receives gains $G_2, G_4,$ and G_5 , whereas MO2 receives only gain G_3 (because MO1 is protected by the honeynet). In a normal-normal condition, no player receives any positive gain, and MO1 pays for the cost of the honeynet.

The payoff matrix reveals two Nash equilibriums, which we find by searching for the best player response, taking as constant the best response of the other player. If MO2 is in an attack mode (greatest payoff = 10), for example, then MO1's attack mode is the one with the greatest payoff (equal to 35). In Table 2, we denote these payoffs (in our example, the pair 35, 10) in bold to denote the Nash equilibriums, attack-attack and attack-normal; these are the conditions that give both players a mutual best advantage.

Analyzing the game's results, we conclude the following:

- In the attack-attack situation, all players have a net benefit due to the honeynet because overall security depends on the security of others. This net benefit could be increased by the proliferation of knowledge gained by MO1.
- The two Nash equilibriums, attack-attack and attack-

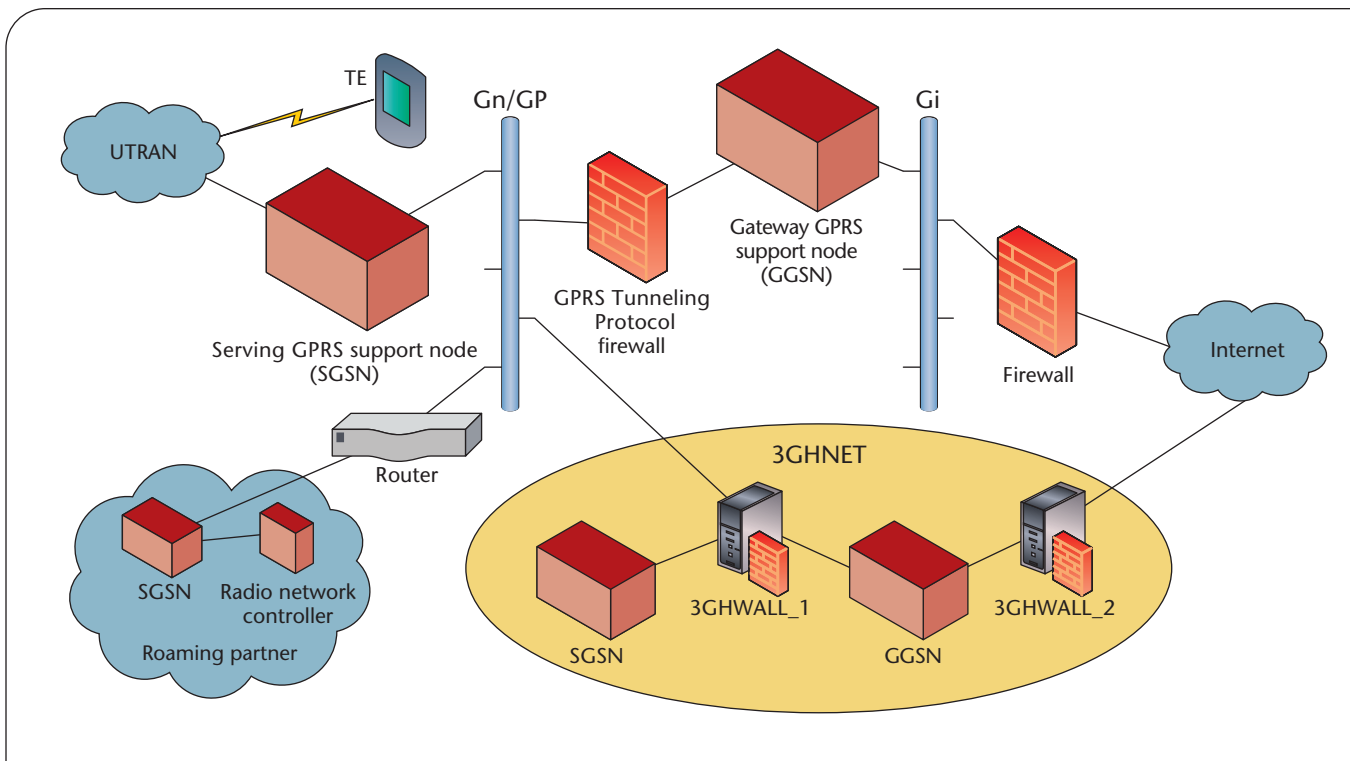


Figure 4. 3GHNET architecture. The honeynet implemented during our study is shown in the yellow ellipse.

normal, reveal that the implementation of a honeynet is useful to both players in either situation.

- If MO2 is compromised and forced to attack, MO1 clearly benefits from implementing the honeynet.
- MO1 gets the highest payoffs by implementing the honeynet, except when security incidents don't arise.

However, the possibility that security incidents won't occur is very small, and when combined with the low cost of implementing open source solutions such as a honeynet, it's quite clear that honeynets are a cost-effective solution for 3G systems. The world of economics and finance offers another consideration: the concept of risk aversion.¹⁷ An entity is risk averse if it will accept a lower expected payoff if it means that it could have a more predictable outcome. Mobile operators are an excellent example of risk-averse entities (the potentially huge business impact from a PS attack versus the low cost of a viable security solution).

The following equation represents security gained as a function of the monetary value an entity is willing to invest in security: $\gamma = f(x)$. If the entity is risk averse, the f function is convex—it will invest more money to have a more predictable result; if entity seeks risk, it won't invest money in security (rather, it will take its chances). Figure 3 shows the corresponding curves.

The dotted lines in the figure indicate the concept of certainty equivalents, which means that if there's a 50 per-

cent possibility a security incident will occur, the first entity (on the left in Figure 3) will invest more money to ensure that countermeasures can address the incident, whereas the second one will take more chances, perhaps by building a less expensive architecture. But in the case of honeynets, $\gamma \gg x$, so the cost of an open source solution such as a honeynet is much smaller than the cost a security incident will incur in a 3G system.

3GHNET's architecture

Due to some uncontrolled network connections in the core network and between its elements and external elements, our study found several critical systems exposed to attack. To address this exposure, a first countermeasure would be to separate the mobile operator's infrastructure into security zones, in which each type of affected element goes in a separate zone. 3GHNET could be implemented in one of these zones; Figure 4 shows its architecture.

3GHNET consists of emulated SGSN and GGSN, which serve as target systems, and two honeywalls with data control and capture functions as prescribed by the Honeynet Project (www.honeynet.org). Because we deployed 3GHNET in a 3G core network environment, we customized it to satisfy some specific needs—to control and capture GTP packets, protect the internal network and external PDNs from compromised SGSN and GGSN emulators, and fully comply with the mobile op-

Table 3. Threat model attack groups implemented per scenario.

SCENARIO ID	TITLE	THREAT MODEL ATTACK GROUP (AG)
A	Attacks against the Gateway Tunneling Protocol	AG1, AG2, AG6
B	Packet Data Protocol denial-of-service attacks	AG5
C	Connection attempts to unauthorized ports	AG4
D	Non-permitted address-range attacks	AG7
E	Over-billing attacks	AG8
F	Compromised node attack	AG3, AG9

erator's security policy. More specifically, 3GHNET's honeywalls have the following characteristics:

- 3GHWALL_1 is a layer-2, non-IP-addressable element that controls and captures data between 3GHNET's emulated SGSN and GGSN and the mobile operator and roaming partner's real ones. 3GHWALL_1 also captures and controls the data flow between the emulated SGSN and emulated GGSN. It deploys Netfilter (www.netfilter.org), which is configured with a set of GTP-specific rules (controlling traffic to and from ports 2152 and 3386), to block all traffic from inside 3GHNET to the core network (or roaming partner). Snort (www.snort.org) serves as an intrusion detection module, and Ethereal (www.ethereal.com) captures and analyzes GTP packets.
- 3GHWALL_2 is a layer-2, non-IP-addressable element that controls and captures data between 3GHNET's emulated SGSN and GGSN and the Internet. This honeywall also uses Netfilter as a firewall to control and log traffic between the two interfaces, Snort as an intrusion detection system for attacks from the Internet, and Snort_inline, another form of Snort, in combination with Netfilter as an IDS for attacks launched from the 3GHNET and targeted at the Internet.

We implemented the emulated SGSNs and GGSNs with an open source emulator called OpenGGSN over Linux operating systems. Mobile operators typically use the OpenGGSN Project's (www.openggsn.org) GGSN emulator as the interface between the Internet and the rest of the mobile network's infrastructure. The OpenGGSN Project has also developed a SGSN emulator suitable for GPRS core network testing. Commercial products—or even better, real GGSN or SGSN systems—might soon be deployed for this purpose.

Security analysis through experiment

To conduct a thorough security analysis of our honeynet's architecture and ability to protect a 3G system, we performed several experiments to emulate various attack scenarios, including attacks from an external PDN (the

Internet) through the Gi interface, as well as attacks from the Gn and Gp interfaces, to emulate compromised SGSN and GGSNs. We based our attack scenarios on our previously described threat model; Table 3 presents an index of AGs implemented per scenario.

Scenario A deployed malformed GTP packets. These attacks generated GTP packets through both an enhanced version of the GTP library in the OpenGGSN tool and packet generators, which produced the content encapsulated in GTP packets. The attacks included malformed GTP headers, invalid GTP payloads (including GTP-in-GTP encapsulation and encapsulation of non-IP-based protocols in GTP) and non-matching addresses between the GTP payload and the assigned address as defined in the PDP context handshake. 3GHNET detected and logged all types of attacks through 3GHWALL_1 and blocked all outgoing traffic destined to the real PS domain.

Scenario B involved GTP denial-of-service attacks implemented by attempting to initiate a great number of PDP contexts. 3GHNET detected and logged all types of attacks and was able to identify and alert system administrators about blocking packets with a specific source address to protect the real PS domain.

Scenario C attacks included attempts to connect to target systems in administration ports and generally any attempt to connect to a port other than the standard GTP ports. Both 3GHWALL_1 and 3GHWALL_2 easily detected these attacks because no local administrator would ever attempt a connection to a non-production system such as 3GHNET.

Scenario D attacks sent packets with non-permitted source or destination addresses by sending users packets with source IP address belonging to SGSN and GGSN address ranges. Both 3GHWALL_1 and 3GHWALL_2 detected and logged these types of attacks.

Scenario E attacks submitted data from a server to an IP address that was re-assigned to a new user, causing the new user to be over-billed. The 3GHNET countermeasure monitored the IP address pool on the GGSN; we specifically configured the honeynet to detect over-billing and unclosed session attacks and inform system administrators about similar attacks in the real PS domain.

Scenario F included attacks that assumed a compromised node and then implemented connection attempts from a roaming partner's unauthorized or compromised SGSNs or GGSNs as well as elements of the local 3G infrastructure. Both 3GHWALL_1 and 3GHWALL_2 detected all types of these attacks.

Figure 2 highlights in red the tree node in which 3GHNET has blocked each attack path. According to the threat model, the first security layer is the establishment or improvement of GTP firewalls. As a response, 3GHNET might directly address an attack targeted to it, as proven by the scenarios we just covered, or indirectly contribute to the improvement of the existing GTP firewall configuration through the knowledge gained by its operation. The second security layer involves the emulation of GGSNs or SGSNs: 3GHNET blocks an attack if it directly targets the emulated GGSN and SGSN, or it can notify a roaming partner about a possible compromise of its infrastructure.

Security in 3G systems should be addressed as a whole because it involves all the elements in the service provision path. To that end, a mobile operator can use our honeynet as

- a laboratory for security officers and engineers to customize, build, and enhance a multilayer security architecture,
- a preventive, detective, and reactive security architecture for the PS domain of a 3G core network, or
- a way to transform a flat architecture into a core network architecture separated into security zones.

Our future research concerns the enhancement of 3GHNET's functionality, based on new attacks we've identified through its operation. Although we didn't investigate it in this current study, if a mobile operator decides to permit traffic through 3GHWALL_1 to study a more precise attack, Snort_inline must be upgraded to help analyze GTP traffic and block malicious packets. Although a specific attacker might not interact with 3GHNET directly, the knowledge and practical experience gained by its operation is a valuable tool in the hands of the security engineer of the mobile operator and also a strong facility for red teams that work toward the identification of new attacks.¹⁸ □

Acknowledgments

I thank the anonymous reviewers for their valuable contributions.

References

1. V. Neimi and K. Nyberg, *UMTS Security*, John Wiley & Sons, 2003.
2. *Security Architecture, TS 33.102*, 3rd Generation Partnership Project, 2006; www.3gpp.org.
3. *Network Architecture, TS 23.002*, 3rd Generation Partnership Project, 2006; www.3gpp.org.
4. D. Wisely, P. Eardley, and L. Burness, *IP for 3G—Networking Technologies for Mobile Communications*, John Wiley & Sons, 2002.
5. *Security Threats and Requirements, TS 21.133*, 3rd Generation Partnership Project, 2002; www.3gpp.org.
6. O. Whitehouse and G. Murphy, *Attacks and Counter Measures in 2.5G and 3G Cellular IP Networks*, @stake press, 2004.
7. K. Kameswari et al., "A Taxonomy of Cyber Attacks on 3G Networks," *Proc. IEEE Int'l Conf. Intelligence and Security*, IEEE CS Press, 2005.
8. W. Donald and L. Scott, "Wireless Security Threat Taxonomy," *Proc. IEEE Workshop on Information Assurance*, IEEE CS Press, 2003; <http://ieeexplore.ieee.org/iel5/8722/27611/01232404.pdf>.
9. N. El-Fishway, M. Nofal, and A. Tadros, "An Improvement on Secure Communication in PCS," *Proc. Performance, Computing, and Comm. Conf.*, IEEE Press, 2003; <http://ieeexplore.ieee.org/iel5/8553/27061/01203697.pdf>.
10. C.J. Mitchell, *Security for Mobility*, ACM Press, 2004; <http://portal.acm.org/citation.cfm?id=995774>.
11. B. Schneier, "Attack Trees," *Dr. Dobbs's J.*, vol. 24, no. 12, 1999, pp. 21–29.
12. The Honeynet Project, *Know Your Enemy: Learning about Security Threats*, Addison-Wesley, 2004.
13. M.J. Osborne and A. Rubinstein, *A Course in Game Theory*, MIT Press, 1997.
14. A. Cournot, *Researches into the Mathematical Principles of the Theory of Wealth*, Macmillan, 1897.
15. J. von Neumann and O. Morgenstern, *Theory of Games and Economic Behavior*, Princeton Univ. Press, 1944.
16. J. Nash, "Equilibrium Points in n-Person Games," *Proc. Nat'l Academy of the USA*, vol. 36, no. 1, 1950, pp. 48–49.
17. M. Rabin, "Risk Aversion and Expected-Utility Theory: A Calibration Theorem," *Econometrica*, vol. 68, no. 5, 2000, pp. 1281–1292.
18. H.T. Ray, R. Vemuri, and H.R. Kantubhukta, "Toward an Automated Attack Model for Red Teams," *IEEE Security & Privacy*, vol. 3, no. 4, 2005, pp. 18–25.

Christos Dimitriadis is a researcher at the University of Piraeus, where he specializes in prevention, detection, and response IT security mechanisms. His research interests include 3G and 4G security architectures, identity management, honeynets, and security protocol design and testing. Dimitriadis has a PhD in IT security from the University of Piraeus and is a Certified Information Security Manager (CISM) and Certified Information Systems Auditor (CISA). He is a member of the IEEE and the Technical Chamber of Greece. Contact him at cricodc@gmail.com.