Research Statement

Guan-Hua Tu
University of California, Los Angeles

My research interests are in **computer networks** and **network security** with an emphasis on the mobile Internet. The current 4G mobile network is a large-scale, global information infrastructure on a par with the wired Internet. It is the only wireless infrastructure that offers wide-area, ubiquitous data and voice services. More and more users have been using it to access the online services through their smartphones on a daily basis. This trend is continuing, and the mobile data traffic is expected to grow almost 10-fold from 2014 to 2019, 3 times faster than the wired Internet traffic.

However, the state-of-the-art mobile network technology is not without limitations and flaws. First, its reliability raises serious alarms under various scenarios of user mobility, intermittent connectivity, and problematic systems operations. The network can be best characterized as usable, rather than dependable. Second, unprecedented malicious attacks towards mobile devices and the infrastructure pose continuous security threats. For example, we have recently shown [6] that millions of Facebook/Twitter accounts can be easily hacked without passwords by exploiting the vulnerabilities of texting services on LTE networks. The fundamental problem is that, the current mobile network technology is the product from the forced marriage of legacy telecom practice and Internet design. It has not been going through rigorous screening in both design and operations by the research community.

My overall goal is to design and prototype a *dependable* and *secure* mobile Internet infrastructure to smartphone users and upcoming Internet of Things (IoT) devices. To this end, my approach is to first look into the operational networked systems, identify the problematic subsystems, quantify their impact, and derive the technology root causes. This requires innovative applications of cross-disciplinary techniques from fields of systems, networks, security, distributed computing theory and data science. The outcome can be directly transferred to carriers, vendors, and standards bodies. The next step is to propose simple yet working solutions in the form of clean-slate design for the upcoming 5G mobile Internet technology and the cellular Internet of Things.

1 Research Contributions

Along the above direction, my research has produced several pieces of concrete results on both network reliability and network security. I next describe each in details.

1.1 Reliable Network Infrastructure

Broadly speaking, the 4G architecture consists of three planes that work in concert to offer mobile data access: control-plane, data-plane and management-plane. My research activity spans all three planes.

Reliability of Control-Plane Protocols via Domain-Specific Protocol Verification [3, 7] Control-plane protocols of 4G networks are more complex than their Internet counterparts. They offer more network utility functions, e.g., mobility support, radio resource control, and device-level security. In research, the problem of verifying their correctness remains largely unaddressed. This is due to the complex interactions (along three dimensions: cross-layer, cross-domain (circuit-switched and packet-switched) and cross-system (2G, 3G, 4G)) and inaccessible network infrastructure and mobile devices. Protocol operations are not readily accessible from carriers, nor from devices in practice.

In this project, we propose to apply domain-specific model-checking techniques for protocol diagnosis. The goal is to uncover design flaws, as well as operational slips. It works as follows. Specifically, we follow standards specifications to model each control-plane protocol as finite-state machines, running at the mobile device and the network infrastructure. We further define common usage scenarios in terms of mobility, access and traffic demand.

Given a set of desirable properties, we can identify candidate instances that violate such properties in the given scenario. Such potential instances are further (in)validated at the operational network. It is done via a phone-based validation method we have devised. This way, we are able to circumvent the closed infrastructure via protocol modeling and phone-based experiments.

Our effort also yields new findings on protocol correctness. We discovered two new classes of problematic interactions among signaling protocols: (1) *necessary but problematic cooperation* and (2) *independent but coupled operations*. They also result in user-perceived performance penalties in the form of temporary out of service, long call setup time, stuck in an old network. We further propose new designs via *layer extension*, *domain decoupling* and *cross-system* coordination to fix such issues.

Interplays of Data-Plane Data and Voice Services [9] The 4G LTE network uses two voice solutions. One is VoLTE, which is based on packet-switched (PS) Internet voice, and the other is CSFB (CS Fallback, which uses the legacy voice solution in 3G networks and switches a 4G user back to 3G to access circuit-switched voice services). In this project, we examine how voice calls affect data service in 4G LTE networks. To our surprise, we found that voice calls and data access interfere with each other. On one hand, voice calls may incur throughput drop (up to 83.4%), transmission halt for seconds, lost 4G connectivity, and application aborts for data sessions. One the other hand, users may miss incoming calls upon turning on data access. It turns out that, though the 3G and 4G systems are designed and operated independently, they do interact with each other via the mobile phone, which runs dual protocol stacks. Improper design of protocols lead to unexpected interference that results in deadlocks and loops in the protocol finite-state operations.

Fidelity of Management-Plane Data Accounting Subsystems [11, 10] Accurate accounting for data usage is a critical utility function on the management plane of 4G networks. Unlike the wired Internet, most 4G networks adopt the usage-based billing, instead of the simpler flat-rate charging, because the used radio spectrum is limited and licensed. Our studies yield two findings: (1) users can be charged for what they never receive; (2) users may obtain data access free of charge. The fundamental problem is that, the current design follows an element-based design without verifying with the end-to-end operation. Any failure along the end-to-end path may trigger inaccurate accounting that differs from what the end user perceives. Moreover, improper practice of policy-based accounting (e.g., free DNS messages) may expose charging loopholes. We believe that the accounting elements should take the feedbacks from front-end base stations (e.g., which have the first-hand experiences to know the data volume delivered to the user device). The carriers have to make policy enforcement complete, especially for data services with differential charging policies.

1.2 Network Security

4G networks provide mobile users with three major network services: mobile data access, voice service and text service. My research in security also targets on the three network services.

Towards Secure Mobile Data Accounting System [12, 8] The 4G network infrastructure uses multiple built-in mechanisms to ensure security, including authentication, key agreement, ciphering and integrity protections for data-plane services. However, we find that the control-plane and management-plane functions are not well designed for secure accounting. First, decoupling of authentication, authorization and accounting exposes the data service to attackers, who may send data packets with spoofed source address. The accounting element further bills the victim instead of the attacker. Second, lack of coordination between the device and the network lets the user be vulnerable to spamming attacks. The device cannot request the network to stop the malicious spamming packets, which have been accounted, unless the user disables his data access. We have verified that attackers can incur any volume of spam traffic to the victim, while the victim may not be even aware of it. We propose secure mobile data charging solution, which charges the *right* user for the *right* volume that (s)he authorizes to use.

Security of LTE Voice Service [4, 5, 1] In this project, we examine the security of both CSFB and VoLTE, the two voice call solutions to LTE networks. Our study shows that, both can be exploited to attack individual users and carrier networks. CSFB may allow for the adversary to activate 2G/3G$\leftrightarrow$4G inter-system switch at the victim phone without consent from the victim. Consequently, mobile users may suffer from up to 91.5% throughput drop through the back-and-forth inter-system switch, or lose 4G connectivity for data access [4]. For VoLTE, the user can gain free and prioritized data access by abusing the VoLTE signaling channel to carry data packets. He also suffers from DoS attacks due to spamming over the VoLTE voice/signaling channels [5]. The vulnerabilities of

VoLTE and CSFB lie in seemingly sound design decisions from the functional correctness standpoint. However, such choices may bear unexpected, yet intriguing implications for security. We further provide an alternative voice solution over LTE [1], which does not only have no security issues of VoLTE but also require less overheads. Its merit is that it retains two major advantages of VoLTE: reusing the the well-tested Internet VoIP scheme at mobile devices, and leveraging the priority service offered by the 4G LTE network to ensure call quality. Such lightweight, secure voice solution would benefit all parties of mobile users, carriers and VoIP service providers.

Insecurity of Texting Service in 4G LTE [6] Texting service (i.e., SMS, Short Message Service) is still popular in 4G LTE networks. The security fences designed for the legacy 3G texting service cannot well protect 4G texting due to the infrastructure shift from CS to PS. Moreover, the security mechanisms and permission control for texting and network interfaces in the mobile OS cannot defend the texting attack launched from the PS domain. Consequently, distributed mobile-initiated texting attack is feasible against a group of mobile service providers (e.g., Facebook, Twitter). The adversary is capable of updating million victims' Facebook pages, adding friends or liking specific page without their passwords, or even donating money without their consent. We then propose solutions to carriers and mobile service providers, and work together with them to fix the problems.

1.3 Impacts

The impacts of our work are multi-faceted. First, our results have been documented in a number of top ACM networking and security conferences, including ACM MOBICOM'12, CCS'12, MOBISYS'13, MOBICOM'13, CCS'14, SIGCOMM'14, CCS'15, and IEEE CNS'15. Second, we have worked with the mobile Internet industry to transfer our results to produce real-world impact. Three major US carriers (AT&T, Verizon and T-Mobile) adopted our solutions to address the security vulnerabilities we discovered, e.g., free data service, data and voice denial-of-service, overcharging, SMS attacks. Millions of US mobile users have benefited from our work. Third, our findings have appeared in several media coverage by MIT technology review, Computer World, Fiscal Times, TheVerge, RCRWireless, etc.

2 Research Plan

I have four immediate directions to pursue in the short term.

(1) Abuse-Resistant Device-to-Device Communication: A key challenge for next-generation Mobile Internet is the limited radio spectrum to serve explosive growth of traffic demand. To address this issue, a promising direction is the device-to-device communication (D2D). Two proximity users can directly communicate with each other without traversing the base station. It thus increases the spectrum efficiency. However, D2D communication also poses challenges to security due to its peer-to-peer data transfer. Attackers can cheat carriers and obtain more data access than reported. In this project, I will devise an algorithm for carriers to estimate the D2D data usage. The research results will be transferred to industry.

(2) Device-Centric Cellular Internet of Things: Current cellular technology cannot meet the diversified demands by Internet of Things. The cellular-connected devices are required to wake up periodically, to check if there is any signaling or data packet for them, and reestablish radio connection and security context accordingly. As a result, it cannot compete with the proprietary cellular IoT technology used by Sigfox in terms of battery lifetime (SigFox IoT modem only wakes up when needed, two AA batteries support it for 20 years) or the volume of signaling. Moreover, most low-cost IoT devices do not afford the nowadays security mechanisms, which require moderate computing power and some necessary hardware support of cellular network (e.g., SIM card), due to the concern of deployment cost and technology gaps. In this project, I explore to place more intelligence to the IoT devices, redesign how IoT devices communicate with the base station, and seek a flexible, lightweight and secure network infrastructure for IoT devices.

(3) Network Security Vulnerability Analyzer: Cellular network security research has taken the empirical approach to security threats. In this project, I plan to devise a Mobile-Internet-specific security vulnerability analyzer with formal checking techniques for cellular networks. I plan to devise *CNetSecVerif*, which examines whether both generic and cellular-specific security properties (e.g., self-disconnect caused by unencrypted paging messages) are violated during various usage scenarios, and generates a full set of security vulnerability analysis report.

(4) Mobile-Technology-Aware Mobile Operating System: Mobile OSes (e.g., Android, iOS) do not fully leverage the mechanisms available from the underlying mobile technology. For example, the mobile OSes are unable to stop the unsolicited (or spamming) packets coming from the network when mobile data service is enabled. The negative impact is that users need to pay for those packets and are vulnerable to spamming attacks. However, this vulnerability can be easily prevented by an existing mechanism from the network, traffic flow template modification. Unfortunately, it is not used by Android and iOS. As a result, I plan to propose a framework that can enable mobile OSes to leverage the available mechanisms from the network, to improve both security and network performance of mobile data service. I will also look for the opportunity to transfer this technology to industry. For example, our iCellular [2] is projected to cooperate with Google for the better user-perceived performance.

3 Outlook

The mobile Internet revolution is still at its early stage. On the network infrastructure side, the upcoming 5G technology aims to provide 1000 times faster wireless access (i.e., 100 Mbps $\rightarrow$ 10 Gbps), support 7 trillion mobile devices for 7 billion users, and save up to 90% energy over radio access by 2020. These stringent requirements call for radical new approaches, transformative technologies and novel security mechanisms. This is exactly my long-term research target.

References

[1] Guan-Hua Tu, Chi-Yu Li, Chunyi Peng, Zenwen Yuan, Yuanjie Li, Xiaohu Zhao, Songwu Lu. VoLTE*: A Lightweight Voice Solution to 4G LTE Networks. accepted to *ACM HotMobile, 2016*.

[2] Yuanjie Li, Haotian Deng, Chunyi Peng, Zengwen Yuan, Guan-Hua Tu, Jiayao Li, Songwu Lu. iCellular: Device-Customized Cellular Network Access on Commodity Smartphones. accepted to *USENIX NSDI, 2016*.

[3] Guan-Hua Tu, Yuanjie Li, Chunyi Peng, Chi-Yu Li, Songwu Lu. Detecting Problematic Control-Plane Protocol Interactions in Mobile Networks. To Appear in *IEEE/ACM Transactions on Networking, 2015*.

[4] Guan-Hua Tu, Chunyi Peng, Chi-Yu Li, Songwu Lu. How Voice Call Technology Poses Security Threats in 4G LTE Network. *IEEE CNS*, Florence, Italy, 2015.

[5] Chi-Yu Li*, Guan-Hua Tu* (*:Co-Primary), Chunyi Peng, Zengwen Yuan, Yuanjie Li, Songwu Lu, Xinbing Wang. Insecurity of Voice Solution VoLTE in LTE Mobile Networks. *ACM CCS*, Denver, US, 2015.

[6] Guan-Hua Tu, Yuanjie Li, Chunyi Peng, Chi-Yu Li, Songwu Lu. New Threats to Messaging-Assisted Mobile Services: Lessons from Individual-Targeted and Large-Scale Attacks Towards Facebook and More Over 4G LTE. *Under submission*.

[7] Guan-Hua Tu, Yuanjie Li, Chunyi Peng, Chi-Yu Li, Hongyi Wang, Songwu Lu. Control-Plane Protocol Interactions in Cellular Networks. *ACM SIGCOMM*, Chicago, US, 2014.

[8] Chunyi Peng, Chi-Yu Li, Hongyi Wang, Guan-Hua Tu, Songwu Lu. Real Threats to Your Data Bills: Security Loopholes and Defense in Mobile Data Charging. *ACM CCS*, Scottsdale, US, 2014.

[9] Guan-Hua Tu, Chunyi Peng, Hongyi Wang, Chi-Yu Li, Songwu Lu. How Voice Calls Affect Data in Operational LTE Networks. *ACM MOBICOM*, Miami, US, 2013.

[10] Guan-Hua Tu, Chunyi Peng, Chi-Yu Li, Hongyi Wang, Xingyu Ma, Tao Wang, Songwu Lu. Accounting for Roaming Users on Mobile Data Access: Issues and Root Causes. *ACM MOBISYS*, Taipei, Taiwan, 2013.

[11] Chunyi Peng*, Guan-Hua Tu* (*:Co-Primary), Chi-Yu Li,Songwu Lu. Can We Pay for What We Get in 3G Data Access? *ACM MOBICOM*, Istanbul, Turkey, 2012.

[12] Chunyi Peng, Chi-Yu Li, Guan-Hua Tu, Songwu Lu, Lixia Zhang. Mobile Data Charging: New Attacks and Countermeasures. *ACM CCS*, Raleigh, US, 2012.