# Project Summary

**Overview**: 5G is emerging and is expected to soon become near-ubiquitous around the world. Hence, U.S. government organizations such as the military and State Department, as well as non-governmental humanitarian aid organizations, and private sector enterprises should take advantage of indigenous 5G networks to eliminate the costs of installing and maintaining an alternate communications infrastructure. However, in many areas of the world, 5G networks are deployed and operated by organizations that are untrusted and potentially hostile to the U.S. In these environments, new security technologies must enable secure operations over untrusted networks. The *GHOST* project protects end-user devices and non-indigenous networking equipment from potential compromise through the use of Trusted Execution Environments. The *GHOST* project prohibits traffic analysis through two mechanisms: the use of Software Defined Credentials; and the use of anonymization techniques to obfuscate communications connections. Finally, the *GHOST* project obscures changes in traffic volume by maintaining a minimum level of "*GHOST*" traffic, and provides for pre-scripted traffic models to confuse and mislead traffic analysis.

**Intellectual Merit**: The *GHOST* project addresses the core intellectual challenge of providing secure communications resistant to penetration and traffic analysis over untrusted networks. The *GHOST* project considers the network as a black box that is assumed to be operated by a hostile agent. Addressing the challenge will yield four intellectual benefits to the research and operational communities. First, the *GHOST* project will deliver technology that will protect end-user devices and non-indigenous networking equipment from penetration and compromise. Second, the *GHOST* project will deliver technology to anonymize or disguise end-user identities and locations, and communications endpoints. Third, the *GHOST* project will deliver technology to overlay normal traffic with "*GHOST*" traffic - essentially network white noise - to obfuscate traffic analysis. Fourth, the *GHOST* project will deliver technology to model and generate "false flag" traffic to further confuse and mislead traffic analysis. *GHOST* technology will benefit end-users of any network, not just untrusted networks. The primary criteria for success of the *GHOST* project will be the ability to obfuscate patterns and prevent traffic analysis.

**Broader Impact**: The impact of the *GHOST* project will be felt in three primary domains; the research and engineering (R&E) domain, the educational domain, and the operational domain. In the R&E domain, researchers and engineers will benefit from development and experimentation of security approaches at higher levels of the software stack than are typically pursued. Moreover, the *GHOST* approach represents a system-of-systems approach to network security which will provide many new opportunities for research and development. In the educational domain, the *GHOST* team's commitment to undergraduate development through the use of undergraduate research assistants and summer internships will promote undergraduate commitment to networking and security. Further, the *GHOST* project team is diverse in both professional disciplines and traditionally underrepresented groups, providing an example of successful team integration. Finally, in the operational domain, the *GHOST* team technology will enable organizations ranging from the U.S. military to private entities to securely operate over indigenous 5G networks, regardless of the politics of the network operators.

# Project Description

## 1 Executive Summary

The proliferation of 5G networks around the world presents an attractive opportunity for the US Department of Defense (DoD) to take advantage of the commercial technology refresh cycle and to reduce the cost of deployment by leveraging these networks. However, many of these overseas networks should be considered to be at least deeply penetrated, if not outright controlled, by near-peer adversaries. And as recently, and very dramatically, demonstrated by the recent death of Russian Major General Vitaly Gerasimov in Ukraine, communicating over an adversary's network in an identifiable manner is an invitation for attack [1]. Thus to be able to leverage commercial 5G investments, novel methods to securely "Operate Through" untrusted 5G networks must be developed.

As a key piece of a larger solution to Operate Through untrusted 5G networks, the University of Colorado Boulder (CU), in partnership with Federated Wireless (FW), proposes to research and prototype 5**G** **H**idden **O**perations through **S**ecuring **T**raffic (*GHOST*), which aims to secure operations over untrusted indigenous networks. *GHOST* specifically aims to: secure user devices and trusted network hardware; frustrate attempts to obtain user identities and locations; obfuscate communications endpoints; and prevent or mislead traffic analysis.

*GHOST* is a multidisciplinary collaboration between academia and industry. The initial Phase 1 *GHOST* team was selected to cover the technical, social, behavioral, and political aspects of communications. The *GHOST* PI, Co-PIs, Senior Personnel, and Collaborators come from Computer Science, Computer Engineering, Political Science, and Applied Mathematics. The team has deep expertise in military communications, 4G and 5G network deployment and operations, security architectures, social network analysis, mass/political behavior, and mathematical modeling. During Phase 1, the team will further analyze the challenges and adapt the membership as necessary to best prototype a robust solution during Phase 2 attuned to the needs and operations of the user community.

- Dr. Keith D. Gremban (PI) brings 30+ years of experience in the defense industry, as well as government experience with the (DoD) and the Department of Commerce (DoC). In addition to wireless communications, Dr. Gremban has experience in social, cultural, and behavioral modeling and technology transition.

- Dr. Tamara Lehman (Co-PI) has expertise in hardware design and hardware support for security. Dr. Lehman has performed innovative research in optimizing hardware design to meet the twin objectives of efficiency and security.

- Dr. Alexandra Siegel (Co-PI) uses original datasets of hundreds of millions of social media posts, text and network analysis, machine learning methods, and experiments to study mass and elite political behavior. Dr. Siegel explores drivers and mitigators of inter-group conflict and intolerance, consequences of repression, and digital dimensions of conflict—including the spread of online hate speech, extremism, and disinformation.

- Dr. Eric Keller (Co-PI) designs and builds secure and reliable networked systems using a cross-layer approach that draws from networking, operating systems, distributed systems, and computer architecture. Dr. Keller is also an entrepreneur, and founded Stateless in 2016 with the mission of simplifying the management of sophisticated and dynamic networks.

- Mr. Salvador (Sal) D'Itri (Co-PI) is Vice-President of Public Sector at FW and Chairman of the National Spectrum Consortium (NSC). Mr. D'itri has extensive experience in the design, deployment, and operation of private 4G and 5G networks, as well as extensive experience with DoD.
- Dr. James Curry (Collaborator) is the former Chair of the Department of Applied Mathematics at CU, and was recently named a Fellow of the Society of Industrial and Applied Mathematicians (SIAM). Dr. Curry is an expert at non–linear dynamical systems, big data analytics, and mathematical modeling.
- Dr. James Neel (Senior Personnel) is Senior Technologist for Federated Wireless where he led their spectrum sharing R&D projects (e.g., DARPA SC2 scenario design, SSPARC, the award nominated 5G SALT tool for UK shared spectrum availability, RFIMS). Named a CIT GAP Top 50 Entrepreneur for Virginia, this former Cognitive Radio Workgroup Chair develops machine learning and distributed cognitive radio designs for commercial and military clients.

The *GHOST* team will attack the *GHOST* challenges with a systematic, collaborative approach that will both advance the state of the art in device and communications security, and provide tangible deliverables demonstrating the utility of the *GHOST* vision, concepts and technologies. Our Phase 1 technical approach will include the following activities: working with the Convergence Accelerator program to understand DoD missions and operational environments; extending and refining the *GHOST* concept and requirements; refining the *GHOST* team and constituent technologies; and prototype development and evaluation. At the conclusion of Phase 1, the *GHOST* team will be finalized, the *GHOST* concept solidified, the *GHOST* technologies selected, and performance metrics and success criteria defined.

### 1.a Intellectual Merit

The *GHOST* project addresses the core intellectual challenge of providing secure communications resistant to penetration and traffic analysis over untrusted networks. The *GHOST* project considers the network as a black box that is assumed to be operated by a hostile agent. Addressing the challenge will yield four intellectual benefits to the research and operational communities. First, the *GHOST* project will deliver technology that will protect end-user devices and non-indigenous networking equipment from penetration and compromise. Second, the *GHOST* project will deliver technology to anonymize or disguise end-user identities and communications endpoints. Third, the *GHOST* project will deliver technology to overlay normal traffic with "ghost" traffic - essentially network white noise - to obfuscate traffic analysis. Fourth, the *GHOST* project will deliver technology to model and generate "false flag" traffic to further confuse and mislead traffic analysis. Ultimately, *GHOST* technology will benefit end-users of any network, not just untrusted networks. The primary criteria for success of the *GHOST* project will be the ability to obfuscate patterns and prevent traffic analysis.

### 1.b Broader Impacts

The impact of the *GHOST* project will be felt in three primary domains: the research and engineering (R&E) domain, the educational domain, and the operational domain. In the R&E domain, researchers and engineers will benefit from development and experimentation of security approaches at lower levels of the software stack than are typically pursued. Moreover, the *GHOST* approach represents a system-of-systems approach to network security which will provide many new opportunities for research and development. In the educational domain, the *GHOST* team's commitment

to undergraduate student development through the use of undergraduate research assistants and summer internships will promote a forward looking commitment to networking and security. The *GHOST* project team is diverse in both professional disciplines and traditionally underrepresented groups, and the team is further committed to broadening participation. Finally, in the operational domain, the *GHOST* team technology will enable organizations ranging from the U.S. military to private entities to securely operate over indigenous 5G networks, regardless of the politics of the network operators.

# 2 Objectives And Significance of the Proposed Activity

## 2.a Convergence Research

The *GHOST* team is attacking the Track G.1 - Non-Cooperative Networks (NCN) problem. We treat the network as a black box in which all traffic may be reported to a potentially hostile agent. The *GHOST* team only has control of end-devices connected to the network, or reachable by the end-devices, such as over a local area network or another external network (which may or may not be NCN). This kind of situation is likely to be encountered in multiple scenarios, many of which arise from operations in urban environments. In particular, operations in so-called "mega-cities" [2] would likely have multiple, co-existing NCN networks. Some example scenarios include:

- Host Nation Military Assistance: The U.S. military is often deployed to aid in maintaining territorial integrity or provide counter-insurgency support. Many political hot-spots in the world have 5G networks that were deployed by organizations sympathetic to, or controlled by, competing or even hostile countries. The secure use of indigenous 5G networks would simplify communications challenges while maintaining operational security.

- Humanitarian Assistance and Disaster Relief (HADR): In the event of a natural or man-made disaster, the U.S. military is often deployed to host nations to provide logistics, medical, public safety, and other support. The secure use of indigenous 5G networks would speed response time and simplify communications with the host nation and other responders, while protecting U.S. force structures, capabilities, and procedures.

- Diplomatic Operations: The Department of State and other U.S. government agencies operate in foreign countries where the secure use of indigenous 5G networks would be desirable. Diplomats and staff require robust communications, which must be kept secure to protect U.S. interests.

- Multi-national Corporations: Corporate communications have become valuable targets of espionage to obtain valuable intellectual property (IP), insight into corporate strategies, and more. The secure use of indigenous 5G networks would enhance the ability of U.S. corporations to compete cost-effectively without concern of exposing corporate secrets.

5G was designed with a greater emphasis on security than previous generations of cellular communications. Encryption of user data packets is required [3]. The *GHOST* team assumes that data is protected, and focuses on other parts of the security problem. The specific challenges identified are shown in Table 1.

The Phase 1 *GHOST* team is multidisciplinary and includes a line up from academia and industry that covers the expertise required to solve the challenges so far defined. As expected, further refinements of scenarios and challenges will be conducted during Phase 1 and the *GHOST* team will be reconfigured as necessary. The sections below outline the technical approach to the challenges identified.

| Challenge | Technology | Approach |
|---|---|---|
| Protect Devices and Trusted Networks | Trusted Execution Environments (TEEs) and Zero-Trust Architectures | Secure kernels in devices and network hardware |
| Protect Subscriber Identity | Software Defined Credentials (SDC) and Internet Anonymizers | Frequently exchange identities in a scrambled pattern |
| Protect User Locations | Location Obfuscation and Internet Anonymizers | Anonymize location patterns of SDC managed identities |
| Protect Communication Connection | Onion Routing and Internet Anonymizers | Peer-to-peer anonymizers and "ghost" traffic |
| Protect Traffic Profiles | Traffic modeling | Inject "ghost" traffic to cover or simulate an operation |

Table 1: Targeted challenges and preliminary approaches.

### 2.a.1 Protecting Devices and Trusted Networks

In order to provide an additional level of security to end-devices before they enter the hostile network, the *GHOST* team will investigate ways to leverage existing technology in modern processors to boost the confidentiality and integrity of the proposed mechanisms (described in subsequent sections). The team will also investigate methods to accelerate the computation of the proposed algorithms without compromising security by leveraging new software level networking functionality via the extended Berkeley Packet Filtering (eBPF). in the next few paragraphs we provide some background to explain the challenges we will address in Phase 1 of the project.

**Threat Model**. The proposed security mechanism is based on the threat model that assumes an adversary that has remote (or physical) access to the machine and can probe the hardware to infer information about the victim program running the network packet processing to reverse engineer the obfuscation methodology. The adversary can run any program they desire on the target machine to subvert the processor to leak secrets through a variety of vulnerabilities (including privilege escalation and physical attacks).

**Trusted Execution Environments**. Trusted Execution Environments (TEEs), such as Intel Software Guard eXtensions (SGX) and ARM Trustzone commonly found in modern processors, can boost the security of end-user devices by isolating the execution of well defined programs and securing data in memory [4, 5, 6]. The idea behind a TEE is that anything coming from outside the chip boundary is untrusted, and that includes the kernel data and code, as a kernel can be taken over by a malicious party and be modified to steal sensitive data. TEE enforce this trusted boundary by implementing integrity verification of data and code and encrypting them once they leave the trusted boundary. This additional security comes at the cost of certain restrictions.

First, programs to be run inside a TEE must have a static binary, and just-in-time compilation is strictly prohibited as the binary needs to be signed with a certificate to verify its integrity. Second, unlike non-secure execution environments, programs running inside a TEE are required to have limited interactions with both other non-secure programs as well as the kernel and the outside world (*i.e.* IO). Finally. TEE programs are required to statically allocate variables within a predefined region in memory, which is considered the secure memory region. Programs running inside the TEE are allowed to access both the secure memory region as well as the insecure memory region but programs outside the TEE are not allowed to access the secure memory region. The

secure memory region comes with additional security features such as integrity verification and confidentiality, in certain technologies like Intel SGX [7].

TEEs also often have the benefit of remote attestation [4, 8]. When using the TEE technology, a program running in a remote device can attest to the security of the processor in which it is running as well as the security of the binary before it runs. Remote attestation makes use of a hardware embedded cryptographic key, machine-only readable, to derive keys that can prove that a machine has the necessary features to be able to run a program securely. For example, Intel processors that have SGX enabled, have an embedded key inside each processor that can prove its identity as a verified Intel processor.

**Leveraging Secure Hardware for Networking Functions**. All of these features of TEEs can be leveraged to improve the security of a network packet processing program running within an untrusted network. The confidentiality and integrity of TEEs can prevent the end-user device from allowing rogue packets to be accepted. Furthermore, the integrity of the binary in the TEE can prevent adversaries from modifying the functionality of the packet processing program. The remote attestation feature also allows trusted end-user devices to verify that they have a secure connection and to prevent man-in-the-middle attacks. Specifically, the Elliptic Curve Digital Signature Algorithm (ECDSA) attestation in server-class Intel processors allows for end-users to define their own attestation services to create a private secure network [9].

Emerging programming models such as extended Berkeley Packet Filtering (eBPF) and eXpress Data Path (XDP) [10, 11], can enable the intersection of secure execution environments and packet processing. To be able to leverage the benefits of TEEs, packet processing programs need to be separated from the traditional networking functions in the Linux Kernel. This separation is needed for two reasons. First to make sure the performance of the networking functions is not impacted by the secure features. Second, the separation will enable the proper isolation of the networking functions and the kernel memory.

XDP is a Linux kernel feature that allows the system to accelerate packet processing without having to incur the cost of invoking the whole kernel stack [11]. An XDP program is normally verified with a Just In Time (JIT) compiler to ensure that it will not violate the rules of interaction with the kernel. Network packet processing, as required by the proposed metadata obfuscation algorithm, can be run within the XDP environment to gain performance as well as security.

To maintain the integrity and confidentiality of the packet processing and metadata obfuscation, the XDP networking function will be run on top of a Trusted Execution Environment (TEE). The benefit of doing packet processing inside a TEE is that the mechanism in which the obfuscation will take place can be shielded from attackers that could potentially inspect the behavior of the end-user device to infer certain characteristics of the program.

**Challenges in running XDP on top of a TEE**. The proposed project will investigate ways to run the obfuscation algorithm and the software defined credentials through the XDP interface on top of a TEE. We expect to encounter certain challenges along the way which will be part of the Phase 1 to enable the deployment of the proposed solutions during Phase 2. Current implementations of TEE do not allow programs to be JIT compiled as XDP requires. One challenge we will tackle in this project is to re-define the interface of XDP so that it is amenable to the constraints of the TEE. One way to tackle this challenge is to incorporate the restrictions of the XDP JIT compiler with the runtime checks that traditional TEEs have.

Another restriction in a TEE is the inability to communicate with the outside world. By default, XDP runs inside the driver of the network card, so this is another interaction that we will have to redefine in order to protect the network functions within a TEE. One potential approach is to define an interface between the two and facilitate a secure communication channel through the memory.

Finally, current TEE implementations have an explicit and statically allocated region in memory

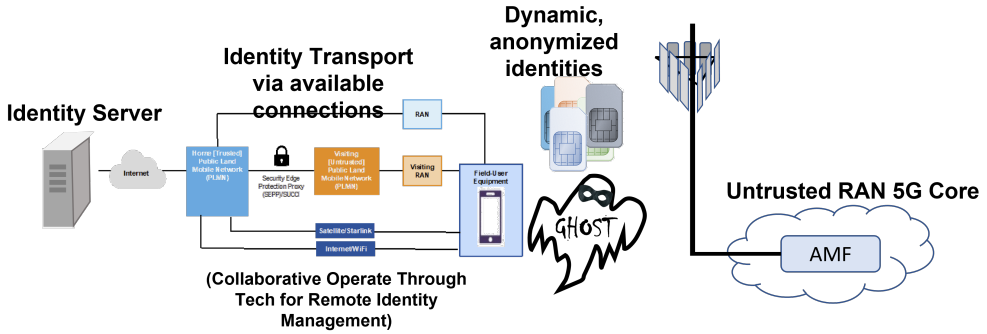



Figure 1: *GHOST* dynamically presents identities and credentials to the indigenous network. These are managed by an identity server connected to user UEs via alternate available Internet routes.

that prohibits Direct Memory Access (DMA). Naturally, the network card driver needs to have the ability to access memory that is also DMA enabled. One way to get around this challenge is to allow the TEE to communicate with the DMA enabled memory region and to copy data into the protected memory region before any sensitive processing is done.

### 2.a.2 Protecting Subscriber Identities

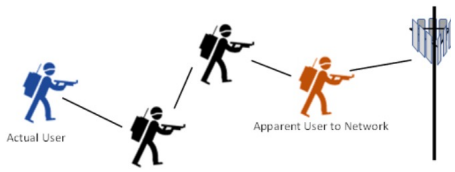
Beyond the associated individual privacy and security issues, mobile network operators (MNOs) have a business interest in verifying that users on the network are who they say they are and only accessing the appropriate services (*i.e.* a paying customer). The MNOs then authenticate users to the 5G network when attaching and then at regular points during communications (*e.g.*, during handovers) based on a collection of unique identifiers for that device (*e.g.*, soldered into an eUICC) or embedded on a removable Subscriber Identity Module (SIM) card. While the more modern embedded SIMs (eSIM) were designed in a way to allow for easy re-provisioning and movement of users across MNOs and support for multiple SIMs, there are a handful of identifiers that attach / remain with the phone including the Embedded Identity Document (EID) (for the eSIM), the MEID (for cdma networks), the ICCID (to identify SIM cards), the IMSI (to identify the subscriber associated with the SIM), and the IMEI (mobile device).

Regardless, while attached to a cellular network, that device / sim / esim combination is uniquely and regularly authenticated for ongoing access, which means that any adversary with access to that network has a unique identifier for the user. However, if those credentials could be defined in software instead of hardware, then a phone / user could identify as any valid (provisioned) user / device / SIM combination that was not currently in use. With the emergence of various academic and DoD-related software defined and open-source 5G UE implementations, software defined credentials (SDCs) appear at a surface level to be a technically feasible approach to anonymize and obfuscate the identity of users Operating Through untrusted 5G networks (as shown in Figure 1). However, the following needs to be established:

1. **Verification of device / user / SIM anonymization** – whether via a fully software defined UE or a via a software-defined SIM [12], the ability to change out the identity presented to the network and observable by the operator needs to be established.

2. **Management of identities** – As simultaneous uses of the same identities are formally disallowed, some process to ensure no duplication of identities amongst the military user pool. Furthermore, the distribution of identities should be scrambled over time for anonymization


(a) Example of regions with distinct traffic patterns.




(b) Example of location obfuscation

Figure 2: High-level overview of user location and identity protection

/ obfuscation. Establishment and maintenance of the pool of identities also needs to be addressed, though modern smartphones expose these identifiers, *e.g.* see the About (iPhone) or About Phone (Android) screen on your phone.

3. **Identity distribution** – To vary identities over time, they need to be regularly distributed to devices, ideally while in the field. Collaborating with other Operate Through Technologies, e.g., the multiple paths for Resilient Communications, will simplify the challenge of remotely managing reconfigurations over a connection that will likely have to be taken down during reconfiguration (restart authentication)

The proposed *GHOST* SDC Phase 1 activities will verify the feasibility of the software defined credentials concept using one of the in-house 5G networks at FW and a software defined UE or software defined SIM – no equipment is planned for purchase, but software will be evaluated and discussions with software-defined SIM vendors will be held. Collaborations with other 5G Operate Through Technologies will be pursued, particularly for connectivity for identity distribution over alternate channels and to align SDC processes with user community expected operations.

### 2.a.3 Protecting User Locations

Cellular networks geo-locate subscribers while connected and smart phones by default collect locations and build profiles of typical user movements (e.g., "home" or "office"). Here, we primarily seek to frustrate the low-level network geo-location processes as that will likely draw undue attention to the users; rather we seek to limit the ability of adversarial network operators to successfully build movement profiles, e.g. identifiable as military users or high value targets.

In practice, this means that the identity pool needs to be managed so that they're not used (or used only consistent with local pattern of life) when communicating from known military bases and from areas / times when a known military operation occurred (an example map is shown in Figure 2a). In Phase 1, we will assess and demonstrate the ability to construct and manage geo-spatial / temporal areas that intersect with the identity pool. We will then collaborate with researchers on this team and across the 5G Operate Through efforts to explore the feasibility of incorporating pattern of life information into this geo-spatial identity management scheme to further frustrate the ability to identify users from patterns of movement.

In Phase 1, the *GHOST* team will also seek out performers on Operate Through Secure MANET to collaborate with as users connecting to the indigenous network via multiple D2D (Sidelink) hops. These connections should be synergistic with obfuscating user location profiles with direct user geo-location.

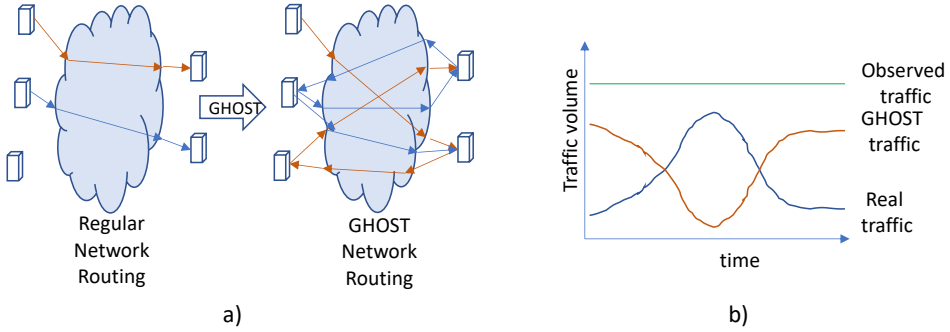



Figure 3: *GHOST* obfuscates metadata and routing to prohibit correlating senders and receivers (left). *GHOST* injects false traffic to prohibit traffic analysis (right).

### 2.a.4 Protecting Communications Connections

Edge devices may appear to the untrusted network as undistinguished edge nodes. However, the connections between edge nodes, along with the volume of traffic into and out of each node can reveal a treasure trove of information about the nodes themselves and the relationships between them. Consider any hierarchical organization. The amount of traffic at each node is roughly proportional to its level in the hierarchy. The connections between nodes reveal information about the reporting structure. To protect the hierarchy and reporting structure, the connections between nodes must be obfuscated, and traffic volume at nodes must be normalized.

Anonymity on the internet has been a research topic for decades. Possibly the earliest work in anonymization was that of David Chaum and the concept of a mix network [13]. In the decades since Chaum, the community has developed a host of anonymizers with different underlying assumptions about the network environment, computing power, acceptable latencies, and threats. Examples include systems like TOR [14, 15], Tarzan [16] and MorphMix [17], among many others.

All anonymizers work in basically the same way. A message from A to B is sent through one or more intermediate nodes, or mixers, with a layer of encryption for each node along the way. At each intermediate node, a layer of encryption is removed, revealing the next stop in the circuit. With a single mixer, many nodes are sending messages in, and many messages are going out, so it is difficult, but not impossible, to determine the source and destination of a particular message. Identifying connections is harder with more intermediate nodes. The primary differences between implementations of anonymizers are in the number of mix nodes available and the path lengths.

The preliminary *GHOST* concept is for a peer-to-peer anonymizing system in which each edge node has the capability to act as an intermediary/intermediate mixer node. Figure 3 illustrates the concept. During Phase 1, through the use of simulation and analysis, the *GHOST* team will explore different mechanisms for selecting and coordinating the use of mixer nodes. Some of the issues we will consider are:

- Schedules and availability - Not all edge nodes will be active all of the time, and activity should be distributed, rather than concentrated in a small number of nodes. We will investigate mechanisms for determining availability and spreading activity across nodes.

- *GHOST* traffic - High traffic nodes are often associated with a higher level in the reporting hierarchy. We will investigate injecting "*GHOST*" traffic to obfuscate such traffic analysis.

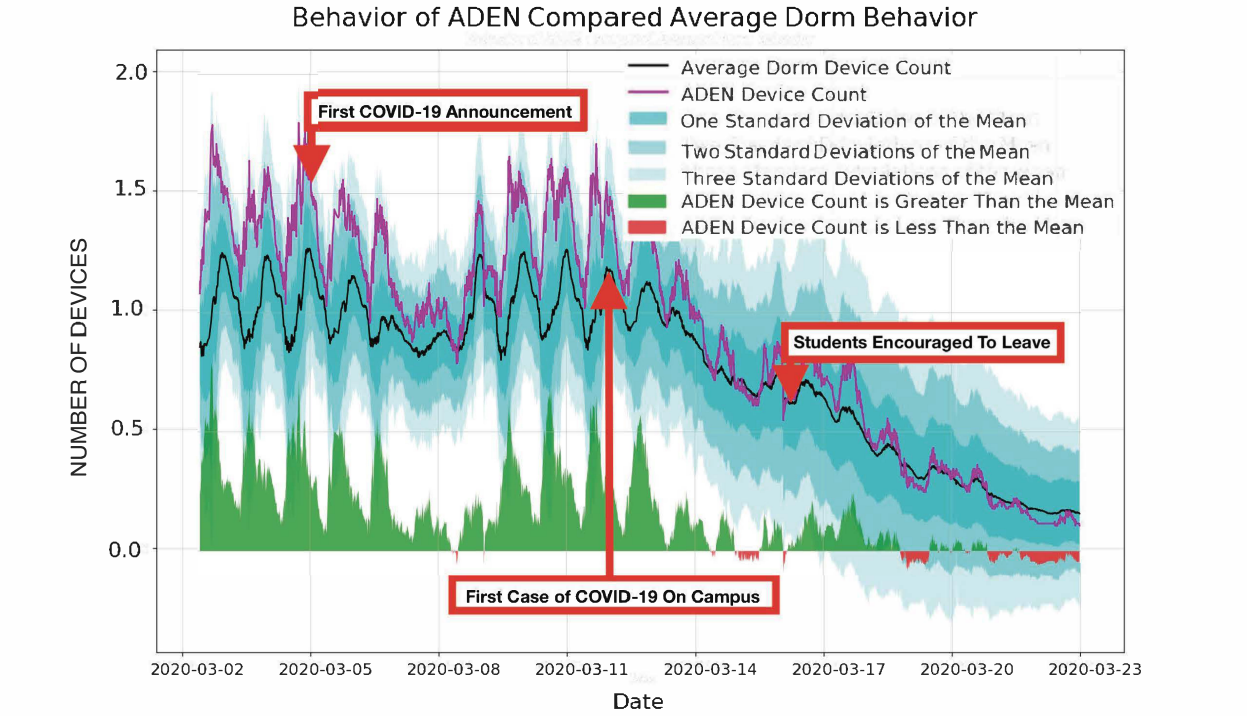



Figure 4: Wi-Fi data: ADEN Engineering dorm compared to average dorm behavior (Spring Semester 2020)

We will investigate prioritizing low traffic nodes as mixers, which will add to their traffic.

### 2.a.5 Protecting Traffic Profiles

Developing models to inject "*GHOST*" traffic to cover or simulate an operation first requires measuring and modeling existing traffic patterns. To do so we will first draw on a real-time collection of Wi-Fi data from dorms, the central campus dining cafeteria, the recreation center, and other buildings on the CU Boulder campus collected since Fall 2019. Members of our team have begun using Singular Spectrum Analysis (SSA), and Non-Negative Matrix Factorization matrix "eigen decomposition" techniques, to analyze these data, classifying clusters of buildings based on their Wi-Fi behavior and highlighting the utility of such models for predicting underlying dynamical systems. Such data can also be used to model events—in the case of a college campus these include holiday breaks, CUPD activities, football games and COVID restrictions—which could be applied to model and predict data usage patterns during diverse events. Figure 4 highlights how Wi-Fi use patterns differ for a particular dorm over a three week period.

To develop models for traffic patterns during common events, we will draw on large-scale social media datasets and Google trends data from various countries. We will identify when bursts occur in the datasets and use unsupervised text analysis approaches including structural topic modeling [18] to determine what types of events produce different patterns. Identifying the types of events that produce large spikes in activity will enable us to simulate *GHOST* traffic to obscure true activity.

| Task | Responsible Parties | Phase 1 Deliverables |
|---|---|---|
| **1. GHOST Technology R&D** | Dr. Keith Gremban (CU) | GHOST Tech Briefs |
| 1.1 Protect Devices and Trusted Networks | Dr. Tamara Lehman (CU)<br>Dr. Eric Keller (CU) | |
| 1.2 Protect Subscriber Identity | Dr. James Neel (FW) | |
| 1.3 Protect User Locations | Dr. James Neel (FW) | |
| 1.4 Protect Communication Connection | Dr. Keith Gremban (CU) | |
| 1.5 Protect Traffic Profiles | Dr. Alexandra Siegel (CU) | |
| **2. System Integration and Testing** | Dr. Keith Gremban (CU) | |
| 2.1 Metric Development | Dr. James Neel (FW) | |
| 2.2 Construct Testbed | Dr. Keith Gremban (CU) | GHOST Testbed Design |
| 2.3 GHOST Technology Integration into Testbed | Dr. Keith Gremban (CU) | |
| 2.4 Evaluate and Refine GHOST Techs and Synergies | Dr. Keith Gremban (CU) | GHOST Performance Evaluation |
| 2.5 Demonstrations and Collaboration | Dr. Keith Gremban (CU) | Demonstrations |
| **3. Collaboration with Other Operate Through Performers** | Sal D'Itri (FW) | |
| 3.1 Innovation Curriculum Participation | All Pis | Curriculum Deliverables |
| 3.2 Team Formation Exploration | Sal D'Itri (FW) | Updated Teaming Plan |
| 3.3 Evaluation of interactions with other secure components | Dr. James Neel (FW) | |
| 3.4 Mission Scenario Identification | Dr. Keith Gremban (CU) | |
| 3.5 Update Research Plan | Dr. Keith Gremban (CU) | Updated Research Plan |
| 3.6 Ph 2 Plan Development | Dr. Keith Gremban (CU) | Ph 2 Pitch, Ph 2 Proposal |
| **4. Broadening Participation** | Sal D'Itri (FW) | |
| 4.1 Outreach and Discussion | Sal D'Itri (FW) | |
| 4.2 Ph 1 Broadening Participation Plan Documentation | Sal D'Itri (FW) | Ph 2 Broadening Participation Plan |
| **5. Project Management** | Dr. Keith Gremban (CU) | |
| 5.1 Contracting / Sucontracts | Dr. Keith Gremban (CU) | Kickoff |
| 5.2 Internal Collaboration and Meetings | Dr. Keith Gremban (CU) | |
| 5.3 Monthly Technical and Finanncial Reporting | Dr. Keith Gremban (CU) | Monthly Reports |
| 5.3 Annual Reporting | Dr. Keith Gremban (CU) | Annual Report<br>Program Income Reporting Worksheet |
| 5.4 Grant Close Out | Dr. Keith Gremban (CU) | Final Project Report<br>Project Outcomes Report |

Figure 5: *GHOST* Program Plan

### 2.a.6 Program Plan and Schedule

The *GHOST* Program Plan and Schedule are illustrated in Figure 5 and Figure 6, both show the systematic development of *GHOST* technology.

### 2.a.7 Evaluation Plan

During phase 1, the *GHOST* team will work on the system integration and testing as well as develop quantitative metrics to evaluate *GHOST* success. System integration and evaluation will start towards the end of year 2022 (as shown in the schedule in Figure 6). The primary criteria for success of the *GHOST* project will be the ability to obfuscate patterns and prevent traffic analysis.

## 2.b Partnerships including a Roles and Responsibilities Table

Table 2 presents an overview of the roles and responsibility of each member of the team, including the type of organization they belong to. Given the interdisciplinary nature of the proposed work all members of the team will be involved in most tasks.

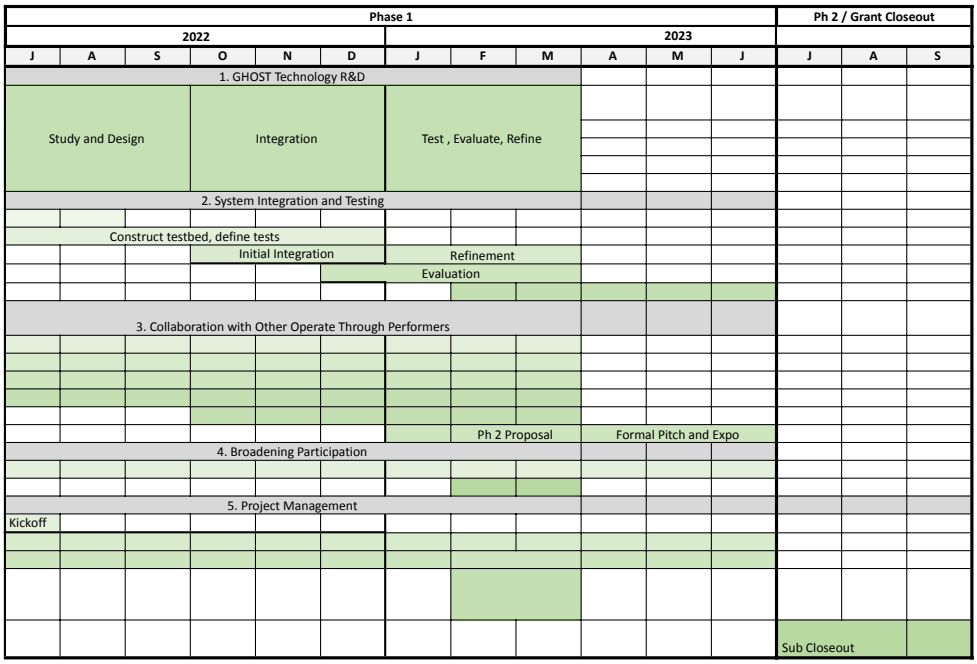



Figure 6: *GHOST* Schedule

| Partner Name | Organization Type | Roles and Responsibilities |
|---|---|---|
| Mr. D'Itri | Industry (Federated Wireless) | FW Sub-contract management and lead the Collaboration and Broadening Participation tasks |
| Dr. Neel | Industry (Federated Wireless) | Lead the development of the Protect Subscriber Identity and Protect User Locations tasks and responsible for Metric Development and Evaluation of Interactions with Other Secure Components. |
| Ms. Johnson | Industry (Federated Wireless) | Project management |
| Dr. Gremban | Academic (CU Boulder) | Overall responsibility for team performance and lead for *GHOST* Technology R&D, System Integration and Testing, and Program Management tasks. |
| Dr. Curry | Academic (CU Boulder) | Participate in the Protect Traffic Profiles task |
| Dr. Siegel | Academic (CU Boulder) | Lead the Protect Traffic Profiles task. |
| Dr. Keller | Academic (CU Boulder) | Co-lead the Protect Devices and Trusted Networks task. |
| Dr. Lehman | Academic (CU Boulder) | Co-lead the Protect Devices and Trusted Networks task. |

Table 2: Roles and Responsibilities

## 2.c Coordination Plan

Key to successful coordination of a multi-disciplinary team is project management. The *GHOST* team is deep in project management expertise. Dr. Gremban, the *GHOST* PI, spent 20+ years in industry and government as a program manager. Mr. D'Itri and Dr. Neel have managed multiple systems integration projects; a significant part of FW's business involves deploying private wireless communications systems. For the *GHOST* project, a professional program manager from FW has been identified and will work with Dr. Gremban to ensure effective management.

The leaders of the *GHOST* project team also understand the challenges of collaboration, es-

pecially across disciplines. The team leaders have extensive experience in working within multi-disciplinary teams, teams composed of both academic and industry partners, and geographically distributed teams, and have developed processes and make use of tools that facilitate collaboration.

The collaboration challenge for *GHOST* is not nearly as difficult as it could be. The PI and several of the Co-PIs are all from the same institution, CU, as are the unpaid collaborators. Dr. Gremban (CU) and Mr. D'Itri (FW) have worked together in the past, as have Drs. Gremban, Lehman, Curry, and Keller.

The collaboration mechanisms that the team will employ will include, but not be limited to:

- Weekly in-person and virtual team meetings to track progress and discuss results. At each team meeting, on a revolving basis, one of the leads will present a detailed discussion of his/her research tasks, progress to date, lessons learned, and the path forward.
- A cloud-based document repository. All team members will be able to access project documentation such as: project plan; project schedule; schematics; processes; and analytic results.
- A cloud-based data repository. Over the course of the project, data and meta-data formats will be documented and the data will be made available to the team.
- A project software repository and version control system (git). All team members will be able to access software remotely.
- A Slack channel will enable near-real-time collaboration during experiments and other events.

## 2.d Deliverables

Table 3 lists the Phase 1 deliverables.

| Deliverable | Task ID | Significance to Phase 2 |
|---|---|---|
| *GHOST* technology briefs | Task 1 | For *GHOST* constituent technologies, formalizes description of, operation and performance to facilitate collaboration discussions with performers and users. |
| *GHOST* testbed design | Task 2.2 | Directly supports *GHOST* testing, evaluation, and initial prototyping. |
| *GHOST* design and evaluation | Task 2.4 | Describes integrated *GHOST* solution CONOPs and initial performance measures. |
| *GHOST* demonstrations | Task 2.5 | Facilitate collaboration discussions and user feedback. |
| Curriculum deliverables | Task 3.1 | Facilitate collaboration exploration to improve *GHOST* for Ph 2. |
| Updated teaming plan | Task 3.2 | Formalization of Teaming plans for Ph 2. |
| Updated research plan | Task 3.5 | Plan to complete and evaluate Ph 2 Prototype. |
| Phase 2 proposal preparation | Task 3.6 | Formalize Plan for *GHOST* Phase 2. |
| Phase 2 pitch development | Task 3.7 | EXPO Participation to refine and improve *GHOST*. |
| Phase 2 broadening participation plan | Task 4.3 | Plan to achieve Broadening Participation Objectives. Improve collaboration with underrepresented groups. |
| Kickoff | Task 5.1 | Orient performers and government on project plan. Set pace of execution. Verify collaboration processes and tools. |
| NSF Programmatic deliverables | Task 5 | Compliance with NSF Program: Monthly Technical and Financial Reports, Annual Report, Program Income Reporting Worksheet, Final Project Report, Project Outcomes Report and other deliverables identified in Contract Award. |

Table 3: Table of Phase 1 deliverables

In Phase 2, if funded, the team will prototype and refine *GHOST* with potential Phase 2 deliverables shown in Table 4. While the exact deliverables will be updated based on collaboration activities and government and user community feedback, the team has previously (e.g., NSC and DARPA projects) successfully followed a similar plan for developing prototypes via rapid initial

development followed by end-user iterations and experiments in parallel with rigorous lab testing, giving us confidence that by March 2025 (fifth prototype iteration) *GHOST* will be a high performing solution suitable for transition to the user community.

| Deliverable | Description | Purpose | Timeline |
|---|---|---|---|
| Phase 2 system testbed | Update the Ph 1 system testbed based on Ph 1 collaboration activities and lessons learned | Controlled test and evaluation of *GHOST* | Dec 2023 |
| Lab prototype | Update Ph 1 prototype | Controlled test and evaluation of *GHOST* | Dec 2023 |
| Field prototype | Prototype *GHOST* software and hardware (SIMs) on suitable smartphone with network connected servers and *GHOST* software | Elicit feedback from users to improve and refine design. Support collaboration exercises with other performers. | Mar 2024 and every three months thereafter |
| Test reports | Documentation of the performance of *GHOST* in terms of communications, anonymization, and ease-of-use | Guidance on prototype revisions | Dec 2023 and quarterly thereafter |
| User guides and training material | Documents that describe the operation and use of *GHOST* | Provide users information on *GHOST* operation for field testing. Revise and prepare for quicker field transition. | Mar 2024 and every three months thereafter |

Table 4: Table of preliminary Phase 2 deliverables

## 2.e Track Alignment

The *GHOST* project will complement the work of other projects in Track G. The challenge the project has undertaken, Track G.1 - Non-Cooperative Networks, restricts the *GHOST* solution to reside on trusted devices. *GHOST* technology does not, in any way, modify the software residing in the target 5G network. *GHOST* obfuscation technology can be applied to augment security on any 5G network, and TEEs can be installed on any compatible edge or trusted network devices. Hence, *GHOST* is complementary to any of the approaches being followed in Tracks G.2 or G.3. In fact, *GHOST* would be a powerful enhancement to any of those solutions.

Dr. Gremban, Dr. Neel, and Mr. D'Itri have extensive experience from industry in collaborating with other organizations on large systems integration projects. For example, Mr. D'Itri is currently leading a project for the DoD 5G Initiative to deploy a private 5G network at a Marine Corps Base, and integrate advanced automation applications into the network. During Phase 1, Mr. D'Itri will lead the Collaboration task and will reach out to other performers to look for opportunities to collaborate. We believe that our technology, as well as our scenario analyses and simulation results will be of interest to Track G.2 and G.3 performers. During Phase 2, we will seek out opportunities for joint experiments to enhance the overall success of Track G.

## 2.f Broader Impacts

### 2.f.1 Overview

The broader impacts of the proposed project can be explained in three domains: research and engineering (RE), educational and operational. In the RE domain, the proposed work will change the way networking functions are conducted by promoting their security as a first-class constraint. To the best of our knowledge no prior team has looked at incorporating concepts of hardware security, such as TEEs, with software defined networks. Furthermore, by addressing the challenge of security over insecure channels, the team will be opening up new questions for the research

community. On the educational side, the team will incorporate experiences for undergraduates, through CU Boulder's opportunities such as the Discovery Learning Apprenticeship (DLA) [19] with specific targets of Black and Native American students, to prepare a diverse next generation of engineers and researchers. Finally, in the operational domain, the proposed solutions will be immediately available for companies, like FW, to be deployed in the field and benefit from being able to operate securely through untrusted channels.

### 2.f.2 Broadening Participation Plan

The proposed *GHOST* work will leverage the existing facilities and programs at CU to recruit a diverse set of students. First, the *GHOST* team will collaborate with the BOLD center at CU (see collaboration letter from acting BOLD Director Amy Moreno) to identify potential undergraduate students to work in related research projects. The BOLD center was originally founded to create a diverse and welcoming environment for engineering students. The BOLD center has close ties with regional Historically Black Colleges and Universities (HBCU), and the *GHOST* team will leverage these connections to identify and recruit outstanding students from these institutions.

Second, the team will partner up with Dr. Ian Her Many Horses (see collaboration letter) to create relationships with student organizations and Tribal Institutions to identify outstanding Native American undergraduate students. Dr. Her Many Horses is himself Native American, and grew up in the Rosebud Reservation. He has served as the Program Coordinator for the Indigenous Alliance Program, a STEM recruitment program for Native HS students. Dr. Her Many Horses has many relationships with Tribal Institutions, and the *GHOST* team plans to leverage those to develop seminars and outreach events to identify outstanding undergraduate students.

Finally, the *GHOST* team will join forces with the research for undergraduate programs at CU (DLA) to provide a sense of community for the undergraduate students working with the team. The DLA program at CU involves undergraduate students in research. Students in this program work on a specific research project, advised by faculty, during the Fall and Spring semesters. Along with the faculty mentorships, the program also offers a structure to ensure the forward progress of the project in the form of mandatory seminars, geared towards improving the students' presentation, writing and reading skills. In addition, the students present their work to their peers several times in each semester, culminating in a college-wide workshop where each student presents a poster.

Members of the *GHOST* team have already had instances of successful interactions with undergraduate students. Dr. Keller and Dr. Lehman are both currently working with one undergraduate student on a research project through the (DLA) program. Dr. Lehman has also advised another student through the DLA program in academic year 2020/2021, and she is still actively working with the same student and about to publish his work in a conference. Dr. Curry is currently working with several undergraduates on research projects in Applied Mathematics.

The undergraduate students will work on a variety of projects, including: developing the XDP programs to run on top of a TEE; developing the testing applications; providing usability feedback for the proposed technology; implementing anonymization technology; and traffic modeling / injection. Undergraduate projects will be shorter in nature and require less expertise while at the same time providing exposure to the proposed technology and learning experiences.

In addition to academic research experiences at CU, both graduate students and undergraduate students will get an opportunity to work in the field with Federated Wireless deploying the proposed solutions. Mr. D'Itri and Dr. Neel have agreed to provide internship opportunities for students to both advance the deployment of the proposed solutions and also improve the diversity in the networking industry. The *GHOST* team will work with undergraduate students involved in the research during Phase 1 to prepare them for internship positions at Federated Wireless in Phase 2,

thereby providing the students with a long-lasting experience.

The success of the Broadening Participation Plan will be measured in two ways: the impact in the career opportunities for students involved and the successful presentation of the project's results at either a workshop or conference. To evaluate the first one, the students involved in the *GHOST* will be asked to provide a yearly report for 5 years after the end of the original relationship. The second measurement will be evaluated by the success of the presentation of the results as well as the quality of the venue where results are presented.

# 3 Results from Prior NSF Support

PI Gremban and co-PI Silbergleit Lehman have one grant together with NSF (ECCS-2030233) in collaboration with Dr. Kevin Gifford. The grant is titled "Passive and Active Spectrum Sharing (PASS)" for the duration 09/15/2020-08/31/2023 in the amount of $1,446,565 to investigate methods for dynamic spectrum sharing. *Intellectual Merit:* The project developed an online RF Open Data Set public repository, published work associated with RF spectrum sensing improving intellectual domain knowledge applicable to the broader field of spectrum sharing, co-organized the NSF NRDZ Workshop-01, and teamed up with the Open Networking Foundation (ONF) to improve the implementation of their Intel SGX management system. The team is beginning to establish requirements and definition for a National Radio Dynamic Zone. *Broader Impacts:* The project will inform U.S. agencies of the requirements for dynamic spectrum sharing, advance knowledge in spectrum coexistence, and disseminate information about spectrum sharing to students.

In addition, Dr. Lehman has one grant from NSF (SHF-2114526) in collaboration with Dr. Jeon from University of California Merced and Dr. Karimian from San Jose State University. The project is titled: "Secure Deep Learning Computing on GPUs" for the duration of 09/2021-08/2024 in the amount of $500,000, of which Dr. Lehman is responsible for $160,000. The project is supporting one graduate student at CU who is investigating microarchitectural defenses to transient execution attacks. No results have been produced yet. *Intellectual Merit*: The project is addressing unique challenges for improving security of deep learning training and inference on both server and edge GPU platforms. *Broader Impacts*: On the education side, the team will incorporate findings of the project into existing courses and assignments. On the outreach side, PI's will recruit a diverse set of students to participate in the project. On the operational side, project findings will improve how security and privacy of GPUs are addressed by industry and government.

Co-PI Keller has received six NSF grants; most relevant to this proposal was "Active Security" (CNS-1406192, $746,537 share, 09/01/14 - 08/31/19), for which he was the PI. In that grant, Dr. Keller explored a new methodology which introduces programmatic control within a novel feedback loop into the defense infrastructure. *Intellectual Merit:* This work has laid the foundation for this novel feedback loop [20], a new framework that is more programmable, and more suited for security applications [21] and [22] (awarded best student paper at Eurosys), demonstrated a new timing attack [23], provided a system for coping with the dangers [23], and introduced a new platform that enables applications to leverage programmable hardware (i.e., FPGA) [24, 25]. *Broader Impacts:* The project is opening up a new set of possibilities in security management of a computing infrastructure, and included undergraduates in the research (Alex Tsankov and Sean Lambert), one of which received a best paper award at SDN World Congress [26].

## References Cited


[1] T. Porter, "Ukraine killed a russian general after he made an unsecured call that gave away his location, report says," *Business Insider*, 2022. [Online]. Available: https://www.businessinsider.com/russia-general-killed-after-ukraine-intercepted-unsecured-call-nyt-2022-3

[2] M. Harris, R. Dixon, N. Melin, D. Hendrex, R. Russo, and M. Bailey, "Megacities and the united states army: Preparing for a complex and uncertain future," Chief of Staff of the Army Strategic Studies Group Arlington VA, Tech. Rep., 2014.

[3] C. Cox, *An Introduction to 5G: The New Radio, 5G Network and Beyond.* John Wiley & Sons, 2020.

[4] I. Anati, F. Mckeen, S. Gueron, H. Haitao, S. Johnson, R. Leslie-Hurd, H. Patil, C. Rozas, and H. Shafi, "Intel software guard extensions (Intel SGX)," in *Tutorial at International Symposium on Computer Architecture (ISCA)*, 2015.

[5] T. Alves, "Trustzone: Integrated hardware and software security," *White paper*, 2004.

[6] ARM, "Arm architecture reference manual," *ARM*, July 2005.

[7] S. Gueron, "A memory encryption engine suitable for general purpose processors," *International Association for Cryptologic Research (IACR)*, 2016.

[8] V. Costan and S. Devadas, "Intel SGX explained," Cryptology ePrint Archive, Report 086, Tech. Rep., 2016.

[9] V. Scarlata, S. Johnson, J. Beaney, and P. Zmijewski, "Supporting third party attestation for intel sgx with intel data center attestation primitives," *White paper*, 2018.

[10] S. McCanne and V. Jacobson, "The bsd packet filter: A new architecture for user-level packet capture." in *USENIX winter*, vol. 46, 1993.

[11] T. Høiland-Jørgensen, J. D. Brouer, D. Borkmann, J. Fastabend, T. Herbert, D. Ahern, and D. Miller, "The express data path: Fast programmable packet processing in the operating system kernel," in *Proceedings of the 14th international conference on emerging networking experiments and technologies*, 2018, pp. 54–66.

[12] Telit, "Simwise datasheet," 2019.

[13] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–90, 1981.

[14] K. Swan, "Onion routing and tor," *Geo. L. Tech. Rev.*, vol. 1, p. 110, 2016.

[15] W.-X. Ding and X.-M. Yin, "Dissection of the multiple mechanisms of tnf-$\alpha$-induced apoptosis in liver injury," *Journal of cellular and molecular medicine*, vol. 8, no. 4, pp. 445–454, 2004.

[16] M. J. Freedman and R. Morris, "Tarzan: A peer-to-peer anonymizing network layer," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 2002, pp. 193–206.

[17] M. Rennhard and B. Plattner, "Introducing morphmix: Peer-to-peer based anonymous internet usage with collusion detection," in *Proceedings of the 2002 ACM Workshop on Privacy in the Electronic Society*, 2002, pp. 91–102.

[18] M. E. Roberts, B. M. Stewart, D. Tingley, E. M. Airoldi *et al.*, "The structural topic model and applied social science," in *Advances in neural information processing systems workshop on topic models: computation, application, and evaluation*, vol. 4. Harrahs and Harveys, Lake Tahoe, 2013, pp. 1–20.

[19] "Discovery learning apprenticeship program." [Online]. Available: https://www.colorado.edu/activelearningprogram/discovery-learning-apprenticeship-dla/discovery-learning-apprenticeship-dla-program

[20] R. Hand, M. Ton, and E. Keller, "Active security," in *Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks*, 2013, pp. 1–7.

[21] J. Sonchack, J. M. Smith, A. J. Aviv, and E. Keller, "Enabling practical software-defined networking security applications with ofx." in *NDSS*, vol. 16, 2016, pp. 1–15.

[22] J. Sonchack, A. J. Aviv, E. Keller, and J. M. Smith, "Turboflow: Information rich flow record generation on commodity switches," in *Proceedings of the Thirteenth EuroSys Conference*, 2018, pp. 1–16.

[23] J. Sonchack, A. Dubey, A. J. Aviv, J. M. Smith, and E. Keller, "Timing-based reconnaissance and defense in software-defined networks," in *Proceedings of the 32nd Annual Conference on Computer Security Applications*, 2016, pp. 89–100.

[24] M. Coughlin, A. Ismail, and E. Keller, "Apps with hardware: Enabling run-time architectural customization in smart phones," in *2016 USENIX Annual Technical Conference (USENIX ATC 16)*, 2016, pp. 621–634.

[25] A. Coughlin, G. Cusack, J. Wampler, E. Keller, and E. Wustrow, "Breaking the trust dependence on third party processes for reconfigurable secure hardware," in *Proceedings of the 2019 ACM/SIGDA International Symposium on Field-Programmable Gate Arrays*, 2019, pp. 282–291.

[26] M. Monaco, A. Tsankov, and E. Keller, "Taking the surprise out of changes to a bro setup," in *Proceedings of the 2016 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization*, 2016, pp. 49–52.

# Facilities, Equipment, and Other Resources

**University of Colorado Boulder (CU)**: CU is the flagship higher education institution in Colorado, and enrolls over 31,000 students, with over 25,000 undergraduates and about5,400 graduate students. While the campus offers a wide breadth of majors, 27% of bachelor's and 62% of doctoral degree recipients earn STEM degrees.

PI Gremban is a member of the Wireless Engineering Research Group (WERG). The WERG research lab is located in the Discovery Learning Center (DLC) at CU, a building designed to facilitate the integration of research and teaching within the College of Engineering and Applied Science (CEAS). Under the NSF SWIFT PASS program, CU has developed a 5G open-source testbed that integrates multiple open-source 5G implementations including Open Air Interface (OAI), the FaceBook Magma Core, and the Open Networking Foundation (ONF) Intel Aether Core with hardware security provision by the Intel SGx secure processing enclave. Additional open-source 5G implementations including Open 5GC and srsRAN will be evaluated during the Phase 1 activities. CU has built a LTE/5G Interoperability Test Lab that is currently (and will continue to be) utilized as a 3GPP 5G Core and UE international interoperability testbed for NASA the Canadian Space Agency (CSA) and for international space agencies participating iin the Consultative Committee on Space Data Systems, CCSDS (https://ccsds.org).

Co-PI Silbergleit Lehman also has a lab in the DLC. Dr. Lehman received an in-kind donation from Ampere Computing in 2021 to build the computing resources necessary to carry out her research activities. The in-kind donation included 8 Ampere eMAG servers each of which included a Lenovo Thinksystem HR330A equipped with 32 ARM cores, 128GB of RAM 1 (8 x 16GB DDR4-2666), 1 SATA SSD with 480 GB space, 1 Dual-port 25 Gb NIC adn 1 1GbE management port. The servers are setup in the Space Science Center (SPSC) and are managed under the Office of Information Technology (OIT). The SPSC has been specifically created to support the research activities of faculty. The datacenter is equipped with state-of-the-art power supply and cooling equipment. The datacenter is kept up 24/7 thanks to the Uninterruptible Power Supply (UPS) and generator backup system. The servers abide by the standard security protocols dictated by the University and sit behind the University network firewall.

*Computer/IT Infrastructure*: The Office of Information Technology Services (OIT) is the primary information-technology provider on the CU Boulder campus, with services for telephony, media, computing and networking. The OIT mission is to provide and promote information-technology services that support the mission of the Campus and provide leadership for the changing information-technology environment. These services include SMART classrooms and clicker technology, computer labs across campus as well as kiosk workstations housed in public campus locations. Students, faculty, and staff enjoy campus-wide wireless access, shared communication networks, calendars and data storage, as well as free walk-in computer and app support. The campus also provides online tutorials through free subscriptions to Lynda.com and expanded internet accessibility through EduRoam.

*Office of Research Integrity*: CU Boulder has research infrastructure in place to ensure that all research is conducted at the highest level of ethical integrity and complies with all state and federal regulations. CU Boulder's Office of Research Integrity oversees research involving human subjects, animal care and use, hazardous materials use and disposal, environmental health and safety, conflicts of interest, and research misconduct investigations. All laboratory members, including undergraduate researchers must complete mandatory training appropriate for their research through regularly scheduled training sessions.

*The College of Engineering and Applied Science*: The Engineering Center comprises 530,000 square feet of classrooms, computing facilities, faculty offices, and research laboratories in an archi-

tecturally distinctive and thoroughly modern building. The center is home to the nation's largest geotechnical centrifuge, ion-implantation and microwave-propagation facilities, several clean rooms, low-turbulence wind tunnels, spectrometers, electron and other microscopes, and a structural analysis facility.

*The Discovery Learning Center*: The most recent addition to the Engineering Center, having opened in October 2002, the DLC offers an additional 45,000 square feet of space to be used for research activities involving collaborative teams of students, faculty and industry partners. This technologically advanced center is home to 11 engineering research centers and is a focal point for a college-wide initiative promoting undergraduate research.

*The Leonard H. Gemmill Engineering Library*: Located in the Mathematics Building at the west edge of the Engineering Village, Gemmill Library is the largest branch of the University Libraries outside of Norlin Library and features more than 155,000 printed volumes and 96,000 microforms.

**Federated Wireless (FW)**: FW is a US-based company headquartered in Arlington, VA with a major engineering office in Boston, MA. As of 2022, FW raised over $150M in strategic and private equity investment from leading US companies including Charter Communications and American Tower. Over 90 employees work in the areas of 5G, network deployment, cloud software development and spectrum engineering. FW's main lines of business are as an FCC-authorized Citizens Broadband Radio Service (CBRS) and Spectrum Access System (SAS) provider and a provider of private 5G wireless networks to commercial and public sector customers. FW is a global provider of spectrum automation services and works closely with international host nation regulators on advancing spectrum sharing. Federated believe the combination of shared spectrum access and security are critical for DoD deployment of 5G networks both in the US and overseas.

*Spectrum Access System Business*: FW is an FCC-authorized SAS provider with over 350 commercial SAS customers and over 100k base station devices connected in real-time to the SAS for spectrum sharing access. Over 50 original equipment manufacturers (OEM) are partners with Federated and connected to the SAS. As a SAS service provider, FW designed, built, deployed and current operates a 200+ network of RF environmental sensors along the entire US coastline to enable shared use between federal incumbents, mobile network operators (MNO) and enterprise customers. Network operations and service delivery are handled from the network operations center (NOC) based in Arlington, VA with a redundant NOC site in Austin, TX. See Figure 7.

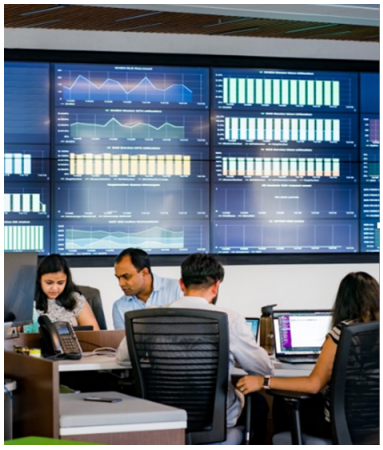


Figure 7: Federated Wireless operates 24x7 NOC

In the international market, FW built and deployed the Shared Access License Tool (SALT) for the UK government under a federal funded program. SALT automates the shared spectrum access to the band N77 (3.8 – 4.2 GHz) to enable rapid deployment of private 5G networks for various business cases. FW was nominated for "Best New Potential Business Application" by the UK 5G Programme office for our partnership in private 5G networks in rural Scotland.

*5G Private Networks*: FW is the prime contractor for the Marine Corp Logistics Base, Albany 5G private network deployed funded under the OSD Research & Engineering 5G Tranche 1 program. FW deployed RAN, 5G standalone core, zero trust architecture using only federally shared spectrum in the band N48 and band N260. This standalone, autonomous network model is directly applicable

to research in standalone 5G network deployments using zero trust solutions. FW is also part of a team deploying an autonomous vehicle, 5G trial using shared military spectrum at US Army Ft. Carson. At McConnel AFB, FW is part of a team deploying CBRS on the flight line for a private, high capacity, zero trust network.

**Other Resources**: The *GHOST* team will collaborate with three individuals - see Letters of Collaboration.

- Dr. James Curry - Dr. Curry is is the former Chair of the Department of Applied Mathematics at CU, and was recently named a Fellow of the Society of Industrial and Applied Mathematicians (SIAM). Dr. Curry will collaborate on big data analytics, and mathematical modeling.

- Ms. Amy Moreno - Ms. Moreno is the Acting Director of the CU BOlD center. Ms. Moreno will collaborate on identifying undergraduates from underrepresented groups, and contacts at Historically Black Colleges and Universities (HBCUs).

- Dr. Ian Her Many Horses - Dr. Her Many Horses is Native American and has served as the Program Coordinator for the Indigenous Alliance Program. Dr. Her Many Horses will collaborate on identifying Native American undergraduates, and contacts at Tribal Institutions.

# Data Management Plan

**Types of Data, Samples, Physical Collections, Software, Curriculum Materials and Other Materials**

*University of Colorado Boulder (CU)* Data collected during Phase 1 will be the results of simulations, analyses, and experiments performed to inform and refine the design of *GHOST* demonstrations and prototypes. The project will produce data in the form of code for the processor simulator, the testing suite, the proposed solutions within the processor simulator, and experimental data. Data sets to simulate network traffic, code to drive the network simulation, and code for anonymization and traffic obfuscation will be developed. All data developed at CU will be stored on servers located on campus and behind the University's network firewall. Data will be accessible to all members of the project.

*Federated Wireless (FW)* FW will leverage an in-house 5G private network, handset devices, and software developers with experience in cellular network software development environments. FW owns and operates all hardware and software needed for this project. Data collected in Phase 1 will be the results of simulations of the behavior of software defined credentials in preparation for *GHOST* demonstrations and prototypes.

**Data and Metadata Format and Content**

*CU* Software produced during the research activities will be stored in the project's main GitHub site. The code will be a mix of C, C++, and Python to conduct the experiments and analyses outlined in the project description. Further, posters and articles produced during the lifetime of the project will be submitted for publication in conferences, magazines, and journals sponsored, for example, by the ACM and IEEE. such publications are published and made accessible via electronic libraries such as IEEE Xplore and the ACM Digital Library. Finally, the material produced for the teaching and outreach activities will be stored on the CU servers, as described above.

*FW* Software produced during this effort will be stored in a GitHub repository within the FW NIST 800-171 and ITAR compliant software environment.

**Handling of Sensitive Data**

*CU* Sensitive data produced by the proposed project will be stored securely per CU security guidelines. All data produced will be stored on servers located behind the University's network firewall. Access to said data will be managed by the CU network control system.

*FW* Data and software created during this effort will be stored in the FW NIST 800-171 and ITAR compliant software environment. The environment is separate from the FW corporate network. Access to the environment will require documented training.

**Software and Data Sharing** Initially, data will only be accessible by users who have an authorized account with the University's network. All students involved in the project, including undergraduate students, will have access to the data. As the results mature, the simulation and testing suite will be made available through the Public access mode of the project's main GitHub account. The proposed activities will produce software that is expected to be of interest to the community. Software will be released publicly through the public more of the project's main GitHub repository through the Open Source Apache v2.0 license. Copyright notices will be distributed as necessary.

**Data Archives and Preservation** Data will be maintained in the CU controlled datacenter environment. The environment will include network addressable storage space protected with RAID-like mechanisms. Data produced in the project will be preserved for at least five years after the conclusion of the project, or five years after the public release, whichever is greater.