Gang Wang

RESEARCH STATEMENT

The explosive growth of user data on the Internet has introduced significant security threats. In recent years, large data breaches and malicious content distribution (spam, malware) become prevalent. With the rapid adoption of mobile and wearable devices, user data now includes a wide range of personal mobile and physical data. It ranges from GPS location traces, to biometrics data, to user interaction data with vehicles and other physical infrastructures.

Meanwhile, humans are playing an increasingly important role in Internet attacks. Whereas most attacks in the past have depended on automated software, today protecting Internet systems is increasingly dependent on a deep understanding of user behavior. First, Internet systems are largely driven by user participation. Whether it is online social networks, content sharing communities or crowdsourcing systems, their functionalities all rely on well-behaved users and high-quality user generated content. In addition, human intelligence is now being used in real-world attacks, to perform tasks that are beyond the capability of software. Examples range from crowdsourced attacks to write fake reviews and create fake accounts, to sophisticated social engineering attacks to infiltrate into enterprise networks. When sufficiently motivated, individual users can overcome most security defenses (e.g., CAPTCHA, template-based spam filter) and produce malicious content that is difficult to detect.

My research centers on the user (human) aspects of Internet security. The goal is to gain a deep understanding of user behavior and its role in attacks and defenses in Internet systems. My research is largely data driven: by collecting and analyzing data from real-world systems, I obtain new insights about attacker behavior in the wild. I also reexamine common assumptions made by existing security solutions and identify unexpected violations in reality. Based on insights from massive data analytics, I develop rigorous and realistic threat models and build practical security solutions to address the emerging threats. Working closely with industry partners (LinkedIn, Renren, Whisper, Microsoft), I evaluate research prototypes in realistic settings and contribute to building production-level systems to protect Internet users.

While I am a PhD candidate, I have successfully applied this methodology to uncover critical and unexpected security threats in various systems including Online Social Networks, Crowdsourcing Systems, Mobile Networks and Enterprise Networks. These results also lead to novel data-driven approaches to combating such threats. My research has appeared in a diverse set of top-tier conferences in security, networking, measurements and human-computer interactions: USENIX Security, NDSS, DSN, IMC, WWW, SIGMETRICS, MOBICOM, MOBISYS, CHI and CSCW. My work has also garnered significant press interest including coverage in MIT Technology Review, Boston Globe, Slashdot, InfoWorld and LA Times. In the following, I will describe my primary research directions and my plans for future research.


Online social networks have eased the communication of billions of users, but are often abused by malicious attacks. Whether it is spam campaigns, phishing or malware distribution [10], attackers can significantly amplify the impact of the attack by creating massive fake identities (or Sybils) to work coordinately. Earlier works on Sybil detection rely on specific assumptions about Sybil behavior. Whether it is the way Sybils build social connection or particular spam content, these assumptions often fail to hold in reality.

Instead of relying on prior knowledge or assumptions on Sybil behavior, my research builds behavioral models based on real-world data. More specifically, I use detailed clickstream traces, which are sequences of time-stamped click events generated by users when they are using the online social networks [7]. The key idea is that Sybil and normal users have different purposes in using the service and thus exhibit different behavior in click patterns. By analyzing large-scale clickstream traces from Renren (China’s Facebook twin, 230M users), I find Sybils exhibit different behavioral patterns from normal users in content clicked, click transitions and click frequency. Based on that, I develop user behavioral models by constructing a similarity graph where each user is a node and the edges are weighted by the similarity of two users’ clickstreams. Partitioning similarity graph produces clusters, each of which contains users of similar clickstream behavior. Since Sybils and normal users behave differently, they can be classified into different clusters.
This approach is semi-supervised. It does not require large-scale ground-truth datasets, which are usually
difficult to collect in practice. Instead, we only need a small set of known good users to label the non-Sybil
clusters for bootstrapping. Without making assumptions about Sybil behavior, we can detect previously
unknown Sybils and attack strategies. Evaluations on real-world datasets show that our method has achieved
high detection accuracy. We also ship research prototypes to our industry partners at Renren and LinkedIn
and contribute to building production-level security systems.

In addition to Sybil detection, clickstream model is also a generic tool to characterize online user behavior.
My recent work combines clickstream analysis with visualization techniques to significantly ease the process
of identifying, tracking, and understanding user behavior in a given system [3]. My on-going work seeks to
extend clickstream behavioral model to broader application domains. Specific projects include user profiling
in anonymous online communities, and large-scale characterization of mobile app behavior.

2. Crowdsourcing and Security
Crowdsourcing has gained great success in aggregating the power of individuals to solve bigger problems.
Early crowdsourcing services (Amazon Turk, oDesk) leverage massive online users to perform tasks that
computers are not good at (e.g., image tagging, transcribing). Recently, research communities (me included)
have investigated the usage of crowdsourcing in many unconventional domains. For example, my works
have demonstrated the effectiveness of using “wisdom of the crowd” to answer to users’ questions [8] or seek
financial advice for stock investment [4]. In terms of security, my works cover topics including using
crowdsourcing to build novel security tools, and the study of malicious crowdsourcing attacks.

Crowdsourced Sybil detection. Attackers continuously evolve as online services adopt stronger defense
mechanisms. Measurement study shows that fake accounts (Sybils) in online social networks are increasingly
sophisticated. Sybils maintain realistic profiles and also perform normal actions, making it challenging for
automated algorithms to recognize them. To identify fake profiles, I explore a novel approach using the
crowdsourced “human intelligence” [9]. The idea is that: by looking at a Sybil profile, people can usually
tell the subtle inconsistencies in her photos or messages based intuitions. We test this idea with a large user-
study based on ground-truth Sybil profiles in Facebook and Renren. The results confirm that humans can
accurately identify Sybil profiles. We then build a crowdsourced Sybil detection system that distributes Sybil
detection tasks to crowdsourced workers from Amazon Turk. We evaluate the impact of incentives and
worker expertise on detection speed and accuracy, and develop an algorithm to optimize performance with
low costs. Our work has received great interests from LinkedIn and Renren.

Malicious crowdsourcing. With the wide recognition of the power of crowdsourcing, attackers also start to
leverage “human intelligence” to carry out attacks. Today, malicious crowdsourcing (or crowdsurfing)
services allow attacker to hire a large group of real-users to carry out malicious campaigns, such as writing
fake product reviews, creating fake social network accounts, and spreading rumors on social media. This
poses serious challenges to existing security mechanisms on the web, since most mechanisms are designed to
stop automated attacks but can be easily bypassed by real users (e.g., CAPTCHA). I conduct the very first
end-to-end measurement study on crowdurfing systems [11]. I have collected data from the largest
crowdurfing services (data over 6 years) to study the system organization, customers, workers, campaigns
and revenue flow. The results show that crowdurfing has turned into an international marketplace with
active services in China, US and India, and hundreds of thousands of real users as workers to perform
malicious tasks; Also, crowdurfing is growing exponentially with individual services reaching a monthly
revenue of multimillion USD.

The measurement results provide new insights to security system design. Instead of assuming all attacks are
massively automated by software, one should include crowdsourced, human-based attacks into the threat
model. In an effort of combating malicious crowdsourcing, I use machine-learning techniques to classify
worker accounts that perform crowdurfing tasks [6]. I build highly accurate classifiers based on
distinguishing behavioral features of crowdurfing workers, and validate their performance using ground-
truth data. Meanwhile, considering that real users are highly adaptive, I build adversarial models to simulate
various countermeasures from crowdurfing workers to evade or manipulate proposed classifiers. This allows
us to proactively anticipate the impact of adversarial attacks on machine learning systems. Recent changes in
crowdvertising services have confirmed that adversarial countermeasures are taking place in practice. Robust
defense against adversarial human-based attacks is still an open problem and require further research effort.

3. Security and Privacy in Mobile Applications

Mobile applications today use the rich smartphones sensors to collect user data (e.g., GPS location) and build
their core functionalities. My work uses empirical methods to study how user data are collected and used,
and examine the key vulnerabilities in this process [1, 2, 5].

An emerging problem is that mobile apps are heavily dependent on user reported sensing data, while lacking
reliable methods to validate data authenticity. This allows attackers to massively inject false data to poison
the system or retrieve sensitive user data in bulks. As a case study, I empirically validate the attack on Waze,
a popular app that collects GPS reports from millions of users for traffic updating and navigation [1]. The
basic idea is that attackers can create a large army of simulated devices to overwhelm the inputs from real
users. This is done by reverse-engineering the communication protocols between the app and server. By
mimicking API calls using simple scripts, attacker can create massive “virtual” devices to run practical
attacks, ranging from creating fake events (e.g., traffic jam) to disrupt user routing, to virtually stalking a
target user wherever she goes. This turns out to be a fundamental problem for a wide range of mobile apps
that rely on massive user GPS as inputs, leading to practical security and privacy attacks. For example, in
anonymous mobile communities (Whisper), such virtual devices can be used to perform massive location
measurements to statistically recover user locations and endanger user anonymity [5].

The measurement results have led to novel approaches to addressing the threats. Specifically, my idea is to
build a location proximity graph, where mobile devices are nodes and edges indicate physical proximity of
two devices. Since it is difficult for software-emulated devices to get into physical proximity to real users,
they will have minimal number of edges connecting to real users in this proximity graph. This allows us to
effectively identify virtual devices in the graph using communication detection algorithms. Simulation results
have shown promising results for this approach [1].

4. Future Directions

Looking forward, I plan to continue to work on data-driven techniques to understand and address security
issues in Internet systems. In the short term (1-2 years), I plan to study the adversarial attacks and
manipulations in E-commerce systems. At the same time, I will be building the groundwork for a long-term
research agenda. My plan is to extend large-scale data analytics to broader security contexts. Specific
projects include ubiquitous crowdsourcing system design, and big data analytics for human centric security.

Adversarial attacks in E-commerce systems. My initial work shows that malicious crowdsourcing has
posed serious threats to a wide range of Internet services. One of the primary targets is E-commerce system
(Taobao, e-Bay, Amazon). To boost the sales of online stores, malicious storeowners are hiring a large
number of real users to write fake product reviews. Despite the defenses in place, attackers have developed
advanced evasion techniques as countermeasure. For example, E-commerce sites usually forbid users from
posting reviews if they did not purchase the product. Recent evidence shows that attackers have learned to
collusively forge purchase record and even make fake shipping to bypass this restriction. In the short term, I
plan to conduct large-scale empirical measurements to understand the sophisticated evasion techniques used
by crowdvertising workers and their effectiveness in practice. Furthermore, I will be developing robust defense
mechanisms for E-commerce systems that are resilient to adversarial attacks.

Ubiquitous crowdsourcing & security. Crowdsourcing has expanded beyond the Internet and become
ubiquitous in the physical world, e.g., house cleaning (TaskRabbit), package delivery (Postmates), taxi
services (Uber) and shared parking (Rover). Future crowdsourcing systems would involve both complex
online user activities and offline interactions with ubiquitous physical facilities such as mobile devices,
vehicles and buildings. To establish trust in the system and prevent malicious attacks, I plan to work on
robust reputation systems that incorporate both online and offline data, and security mechanisms to
continuously monitor the behavior of crowdsourcing participants and detect malicious actions in real-time. Another direction of interest is to explore fundamental design choices for crowdsourcing systems to reduce malicious behavior. The initial step is to understand the tradeoffs of competition and cooperation among crowdsourcing participants. Existing systems (e.g., Amazon Turk) implement strong competitions by default, which however makes it extremely difficult for newcomers to survive and inevitably foster malicious behavior. Future research will explore novel designs to reduce malicious competition and improve the overall efficiency with structured cooperation.

**Big data in human-centric security.** In the long term, as computations are increasingly human-centric, future security systems will be having more direct and intimate interactions with users. A successful security system should be usable in the hand of large-scale online users. I believe big data analytics can make a difference in the design and deployment of usable security systems. On one hand, by collecting and analyzing large-scale data on security system usage, I seek a deep understanding on user-level misuse and misconfigurations of security systems, and explore key design flaws. On the other hand, I plan to collaborate with system and HCI researchers to build novel data-driven security mechanisms that offer high-level transparency and usability. This includes intelligent underlying algorithms to identify security threats from continuous data analytics, and advanced data visualization techniques to help users fully understand the emerging threats to make informed security decisions.

**References**


