TCSN Newsletter – Inaugural Issue – December 2017

Social Networks Technical Committee

Editor: Prof. Damla Turgut

WTC website	http://sn.committees.comsoc.org
WTC officers	Chair: Prof. Kwang-Cheng Chen
	Vice-Chair: Prof. Neeli Prasad
	Secretary: Prof. Jelena Misic
	Information Officer: Dr. De-Nian Yang
Newsletter editor	Prof. Damla Turgut

For information regarding the Newsletter, please contact Prof. Damla Turgut at turgut@cs.ucf.edu.

CHAIR'S MESSAGE

When social media dominates the traffic over the Internet and mobile communication networks, there are further insights and engineering that could be developed based on understanding social networks in depth. Such interplay between technological networks and social networks have so many different aspects to inspire IEEE Communications Society members toward further frontier of communication technology and benefits of human society. Under such background, Technical Committee on Social Networks (TCSN) has been established since 2016, after incubation as a sub-committee in Emerging Technology. When we get to two years old, we are launching the TCSN Newsletters to allow more fluent exchange of vision, ideas, and technological opportunities, in addition to website and social media platforms. We have to appreciate remarkable volunteers at TCSN to make this inauguration issue come true. Last but not the least, we wish TCSN Newsletters serving an effective means for this exciting multi-disciplinary knowledge on social networks to blend humanity and technology in an even better way. Most important, please continue your interest in social networks and actively participate or initiate more volunteer services to TCSN and IEEE Communications Society.

Best wishes,

Kwang-Cheng Chen, Chair, TCSN, 2016-2017

UPCOMING CONFERENCES & CFP FOR SOCIAL NETWORKS TRACK

IEEE Globecom 2018: December 9 – December 13, Abu Dhabi, UAE
IEEE ICC 2019: May 29 – May 24, Shanghai, China

Social networks have become prevalent forms of communication and interaction on the Internet and make up an increasingly part of the network traffic. As a result, social networks have attracted significant research interests in a large number of related areas. Social networks have traditional been studied outside of the technological domains, but focus is now changing towards networking challenges such as cloud, privacy, data analytics, etc. while still keeping the social perspective such as focusing on improving quality-of-life. The interplay between social networks and technological networks such as mobile networks and mobile computing is becoming still strong and many areas are still to be exploited.

TCSN Newsletter – Inaugural Issue – December 2017
Social Networks Technical Committee
Editor: Prof. Damla Turgut

SECURITY IN SOCIAL NETWORKS

MOHSEN GUIZANI, FELLOW OF IEEE

PROFESSOR AND CHAIR, ECE DEPARTMENT

UNIVERSITY OF IDAHO, ID, USA

We have all heard about the recent security breaches targeting big entities such as Equifax, Yahoo, LinkedIn, and Federal Organizations such as DNC. These breaches have compromised millions of individuals' data such as SSN, date of birth, and credit history. Social networks have become a primary tool in the day-to-day communication and networking. This becomes the new target in the security war. Here, we will attempt to highlight the common breaches that can cause havoc in social networks and discuss ways of protecting your personal data.

There are numerous benefits in sharing and communicating through social networks. Sites like Facebook, Twitter, Google +, and many others bring us together in the digital age. With the benefits come many risks. Historically, social networking sites were not prone to hackers. Recently, social network platforms have been built in ways that peak the interest of hackers. Users' increased personal data input can become a big risk with a simple click of a disguised advert link. It is important to take extra precautions to make sure personal information does not get into the wrong hands.

To keep yourself and your information safe, pay careful attention to your online activity. Avoid posting personal information about your bank account(s), full address, birthdate, and your children's personal information. You should also avoid clicking on email links that request personal information received from people you do not know. Before clicking on anything, be sure you know where it is coming from. Some of these emails contain attachments, that may have embedded malware using "rootkits" that are more difficult to remove even after cleaning out your computer/smart device(s). In addition, protect your identity by having strong passwords and be careful with your status updates; post less information on your social accounts—the lesser the better!; avoid posting specific travel plans until after getting back home; be selective on status updates by selecting certain groups (e.g., family); and do not ignore any security settings or updates that can always strengthen the privacy of your information.

These simple steps can ensure that you enjoy communicating on social networks without the risks of compromising your personal information.

TCSN Newsletter – Inaugural Issue – December 2017
Social Networks Technical Committee
Editor: Prof. Damla Turgut

NEXT GENERATION AUTOMOTIVE CYBERSECURITY WITH SOFTWARE DEFINED PERIMETER AND BLOCKCHAIN

MAHBUBUL ALAM, CTO AND CMO, MOVIMENTO GROUP

JUNAID ISLAM, CTO, VIDDER

The emergence of autonomous vehicles is radically changing the automotive business. This change is bringing in new revenue generation opportunities for the whole industry, but with it, also new risks - specifically cybersecurity. Since autonomous vehicles are completely dependent on connected software for all aspects of their operation, they are vulnerable to a broad spectrum of cybersecurity attacks. As we see in the news every day, even well-established sectors like the financial industry and government agencies are still struggling to deal with the same issues. Subsequently, the automotive industry will actually have to leapfrog existing approaches to cybersecurity to ensure that all existing threats are mitigated but also that future "unknown" threats are prevented. Automotive cybersecurity is much more than ransom, data breach, stolen personal records, etc. - it is about the safety of our lives!

The recent sanction of an automotive-specific cybersecurity bill in the US congress, H.R. 3388 also known as the "Self Drive Act", and the Senate's advancements on the AV START Act have sent a clear signal that the automotive industry needs to get serious about cybersecurity. The immediate security risks to connected cars and long-term risks to autonomous vehicles must be addressed. The "Self Drive Act" outlines the cybersecurity plan for autonomous driving systems.

Traditionally, the automotive industry only adopts mature technology. Unfortunately, the rapid pace of software development requires the automotive industry to become more innovative with respect to how it views software. More importantly, the dramatic increase in cybersecurity attacks demands cooperation among OEMs, Tier-1 suppliers, software developers and cybersecurity firms at a scale that has never been reached before. Today's automotive cybersecurity solutions in the marketplace are at best an after-thought. There are still many unanswered questions including how to safeguard internal vehicle systems from attacks, ensure data integrity while also providing data privacy and secure vehicle-to-cloud communications in millions of vehicles that each supports hundreds of ECUs, sensors, domain controllers, radars, LiDAR and ADAS. In order to deliver cybersecurity solutions to address these specific questions for connected and autonomous vehicles, a number of factors must be considered such as scaling globally to a massive number of vehicles, detecting software tampering and malware, support an array of telematics, information and safety applications, enabling precision access control to vehicle software suppliers and meeting regional safety, privacy and driving regulations.

Fortunately, there are two new emerging technologies, Software Defined Perimeter (SDP) and Blockchain, that offer a path forward. SDP enables the provisioning of secure communications between the software process within the vehicle and cloud-hosted applications while Blockchain enables secure messaging. By combining the any-to-any connectivity of the SDP with the scale of the Blockchain, an efficient cyber security model for connected and autonomous vehicles can be created.

In order to further provide secure connected and autonomous vehicles in a systematic manner and provide the required safety, a number of practices should be adopted:

1) Incorporate an industrywide Automotive Cybersecurity Lifetime (from cradle to grave) Compliance Certification program. Make cybersecurity a mandatory part of a vehicle's product development process.
2) Establish a joint automotive cybersecurity taskforce that is responsible for proactive prevention, mitigation and correction of threats and attacks.
3) Provide regulatory agency access to vehicle metadata (non personally identifiable information) for random cybersecurity compliance checks and validation.

What is a Software Defined Perimeter (SDP)?

SDP is a new approach to cybersecurity that is designed to provide on-demand, dynamically provisioned secure network segmentation, that mitigates network-based attacks, by creating perimeter networks anywhere in the world, whether it is in a cloud or in a data center. The architecture comprises of three main components:

(1) Virtual Gateway: A SDP virtual gateway is deployed in a cloud, data center or a connected gateway in the vehicle depending on the use case. This SDP virtual gateway combines the functions of a Firewall, VPN and application layer gateway in a single virtual appliance by only allowing approved software on authorized devices to connect to protected applications inside the vehicle as well as to the cloud.
(2) Client: To allow vehicle software processes to connect to protected applications, they must utilize the SDP client which can be embedded inside e.g. an over-the-air (OTA) software management and data client. This SDP/OTA client has three distinct purposes. Firstly, it allows the automotive policy engine to determine the vehicle identity. Secondly, it allows the remote analysis of software and system processes to detect the presence of malware. And lastly, it provides a secure application layer connection between a software process or ECU inside the vehicle to a software process on a cloud application server.
(3) Controller: Tying the SDP/OTA client and gateway together is a controller. The SDP controller functions as a hub between the client and the gateway as well as external policy systems.

The SDP's interlocked security controls protect software systems within a vehicle and their data from cybersecurity attacks. All SDP transactions are cryptographically certified to mitigate real time tampering while the architecture scales to millions of vehicles supporting billions of software modules and ECUs.

What is Blockchain?

Blockchain, also known as Distributed Ledger Technology (DLT), is a decentralized database for ledgers and transactions. Bitcoin, also known as cryptocurrency, is one of the most famous and widely adopted global virtual currencies in the world and is based on Blockchain. Users gain access to their Bitcoin balance using their private key.

Being immune to a single point of failure and security issues provides a lot of advantages to Blockchain compared to traditional databases. The main advantages of the Blockchain are its immutability, scalability with data security, high data integrity, super transparency (all nodes have visibility into every messaging/transaction metadata) and its ultra-low cost per message/transaction making it very suitable to e.g. micro-payments. Deployments of Blockchain can be either public or private, where, in a public Blockchain (permission-less), any node on the Internet can read from and write to the ledger with

appropriate application whereas, in a private Blockchain, all the nodes in the network are known and have explicit permission to read and write the ledger.

The above-mentioned Blockchain characteristics make it ideal for automotive use cases and OEMs could use a private Blockchain as a platform to enhance their overall cybersecurity for vehicles, validate software bills of materials, enable cost effective micro-payment, strengthen identity management and improve data validation. Examples include pooling of data from vehicles, fleet management, optimize business processes, enable peer-to-peer mobility sharing capabilities that can all disrupt existing business models and improve overall operations.

Combining Software Defined Perimeter and Blockchain for Automotive

Blockchain enable secure messages that can carry a wide variety of payloads from the status of sensors to the delivery of private encryption keys while an SDP provides secure in-vehicle and Internet links. Thus, blockchain messages can be used by ECUs to signal management systems on their status. If a situation requires a secure bi-directional link, an SDP connection can be provisioned from a vehicle-to-cloud resource and, once set up, Blockchain can be used to transmit messages between internal vehicle systems. The combination of SDP and Blockchain technology creates a system that is very lightweight and scalable, and yet has the ability to create secure enclaves when required. In addition to supporting telematics and safety applications, this Blockchain/SDP platform can also support multiple cryptocurrencies such as Bitcoin or Ethereum and thereby be a critical digital payment foundation for the automotive ecosystem.

A simple, but powerful example, of how short Blockchain messages and SDP connections complement each other, is the challenge of driving an autonomous vehicle in the snow. As an autonomous vehicle drives through a snowstorm, it can continuously send Blockchain status messages to cloud-based safety monitoring systems. However, if the vehicle gets stuck in the snow and is unable to dislodge itself, a secure SDP connection can be provisioned which will backhaul all the vehicle image sensors to a specialized cloud application for processing.

Key Takeaways

Both SDP and Blockchain represent the cutting edge of technology. For example, Gartner listed SDP as one of the most important new technologies in 2017 to reshape the enterprise market. Similarly, Blockchain is being adopted as a secure messaging protocol in a wide variety of applications due to its low cost and high scalability. The automotive industry could adopt both technologies as a foundation for secure OTA software/firmware/content updates, secure data exchange and autonomous driving communications. Both Blockchain and SDP are open license free public domain standards and both concepts are proven in large-scale critical deployments in areas such finance and tele communication. This restriction-free model means that there is no barrier for the automotive industry to adopt and innovative on top of them.

With attacks rising every year, cybersecurity has become one of the most important focal points for the automotive industry. A disruptive approach must be incorporated to battle the threat of against cybersecurity attacks that are becoming more sophisticated each day. With the Blockchain-based SDP, OEMs have a unique solution that can empower the global automotive industry to secure connected cars and autonomous cars with confidence.

IEEE COMMUNICATIONS SOCIETY

TCSN Newsletter – Inaugural Issue – December 2017

Social Networks Technical Committee

Editor: Prof. Damla Turgut

SOME THOUGHTS ON SOCIAL NETWORKING FOR RESEARCHERS AND ACADEMICS

DAMLA TURGUT

ASSOCIATE PROFESSOR OF COMPUTER SCIENCE

UNIVERSITY OF CENTRAL FLORIDA, USA

We are all aware of the power of networking in advancing our carreers. Knowing people and being known is an important aspect of the research work. Following our social links, we can gain knowledge about the recent trends of our chosen field, we can publicize our achievements, we can find information about research grants, open positions or people willing to collaborate with us. This reliance on the web of personal connections is not something new - scientists were communicating with each other across countries and continents since the middle ages.

Social networking websites had significantly accelerated this process. The companies owning these sites (Facebook, LinkedIn/Microsoft, Twitter, Tumblr/Yahoo and so on) are strongly interested in encouraging participants to share as much as possible about their personal, and professional lives. This represent a great opportunity to extend the reach of our networking - it is also fraught with danger. Without an attempt to completeness, in the following, I will present some thoughts about what a researcher should or not do on social networking sites.

DO: Share your published papers, conference presentations, invited or keynote talks. We are all proud of our work and want our papers and presentations to be known (and cited!). So it is a good idea to share your papers on the social networks. This is an alternative to the now traditional “publications” page on personal and institutional websites.

DO NOT: Publish confidential information, or data from which confidential information can be inferred. For instance, don’t tweet “Having a great Korean barbeque with my fellow panel members as #NSFPanelOnSocialNetworks” - as you are breaking the confidentiality contract you signed just hours before. And, by the way, a selfie in front of the recognizable Korean barbeque place in front of the NSF building is just as bad.

DO: Be a good citizen of social media sites. “Like”, “applaud”, “upvote” worthy postings - this makes the social networks more useful and relevant to everyone.

DO NOT: Mix personal and professional postings. Obviously, all of us have private pursuits and professional pursuits. Some people successfully mix these together - for instance, Einstein was known to sometimes play the violin when invited for talks. But for many of us, we want to present a professional image to our professional network, and a more relaxed version of ourselves to our friends. So, separate the cute pictures of your doggie from the postings announcing your papers. Use the features of various social networks (circles, friend groups, lists and so on) to target your posting to your intended audience. This applies even if the personal postings are not embarrassing: there is nothing wrong with your dog - only if people come to your site for research news and they have to wade through long pages of cute pictures first, the professional impression might be diminished.