Decapitation via Digital Epidemics: A Bio-Inspired Transmissive Attack

Pin-Yu Chen, Ching-Chao Lin, Shin-Ming Cheng, Hsu-Chun Hsiao, and Chun-Ying Huang

ABSTRACT

The evolution of communication technology and the proliferation of electronic devices have rendered adversaries powerful means for targeted attacks via all sorts of accessible resources. In particular, due to the intrinsic interdependence and ubiquitous connectivity of modern communication systems, adversaries can devise malware that propagates through intermediate hosts to approach the target, to which we refer as transmissive attacks. Inspired by biology, the transmission pattern of such an attack in the digital space much resembles the spread of an epidemic in real life. This article describes transmissive attacks, summarizes the utility of epidemic models in communication systems, and draws connections between transmissive attacks and epidemic models. Simulations, experiments, and ongoing research challenges on transmissive attacks are also addressed.

INTRODUCTION

In recent years, researchers have successfully borrowed several biological mechanisms from nature for devising efficient protocols and understanding their performance via the associated mathematical models, especially for cyber security in communication systems [1, 2]. Inspired by epidemiology, this article investigates an emerging attack pattern, *transmissive attack*, featuring heterogeneous propagation paths and specific targets. Analogous to the spread of epidemics in nature, malicious codes act as viruses that are capable of infecting hosts (i.e., electronic devices) via various communication resources, and they can be stealthily transported by intermediate hosts to reach the primary hosts (i.e., targets), which is similar to the biological mechanism known as *host specificity*.

Inevitably, the proliferation of electronic devices equipped with communication capabilities and the penetration of the Internet of Things have created ever increasing security threats that we call *digital epidemics*, which may be even more vital than actual transmissive diseases like Dengue fever, ebola, and SARS due to their cyber transmission and dormant operation nature, and their induced loss in properties and privacy. It is worth mentioning that although the fragility of modern communication systems may seem to be shocking news to the world, the severe consequences caused by digital epidemics have been foreseen by researchers [3–5]. In the past two decades various advanced communication technologies, such as cellular systems and wired and wireless networks, and tremendous user activities, such as online social networking and mobile applications, have constituted a heterogeneous but ubiquitous network among users and devices around the globe, which is known to be a complex communication network [6] or a generalized social network [5]. Malicious codes are able to exploit these heterogeneous communication paths and intrinsic system interconnectivity for propagation, and thereby compromise more devices.

By investigating recently discovered attack cases and system vulnerabilities, we present an emerging attack pattern named *transmissive attack*, where an adversary can leverage diverse communication paths and common communication protocols (e.g., the Internet of Things) to indirectly compromise a target (or a set of targets) that cannot be directly accessed by the adversary.

Furthermore, in order to increase the possibility of reaching the target, transmissive attacks may camouflage their activities to elude detection rather than indiscriminately infesting as many hosts as possible. The specificity to targeted attacks and heterogeneity in propagation paths distinguish transmissive attacks from well-known Internet worms such as Code Red, which only exploits a single propagation resource (the Internet) and features indiscriminate attacks.

Figure 1 illustrates several possible means for the adversary to access the target.[1] Consider the target to be a personal computer in an enterprise that is granted access to private employee/customer databases or confidential corporate files, and all external networking connections to the target are prohibited. If the target is connected to other internal machines that connect to the outside world, the adversary can eventually reach the target by successive propagation. Pessimistically, even if all connections from other internal machines to the target are prohibited, the adversary can still manage to approach the target by compromising the authorized user's electronic devices, such as portable storage devices, wearable

This article describes transmissive attacks, summarizes the utility of epidemic models in communication systems, and draws connections between transmissive attacks and epidemic models. Simulations, experiments, and ongoing research challenges on transmissive attacks are also addressed.

Pin-Yu Chen is with the University of Michigan; Ching-Chao Lin and Shin-Ming Cheng are with National Taiwan University of Science and Technology; Hsu-Chun Hsiao is with National Taiwan University and CTTI, Academia Sinica; Chun-Ying Huang is with National Chiao Tung University.

[1] A detailed attack scenario is provided in the supplementary file, http://arxiv.org/abs/1603.00588

0163-6804/16/$25.00

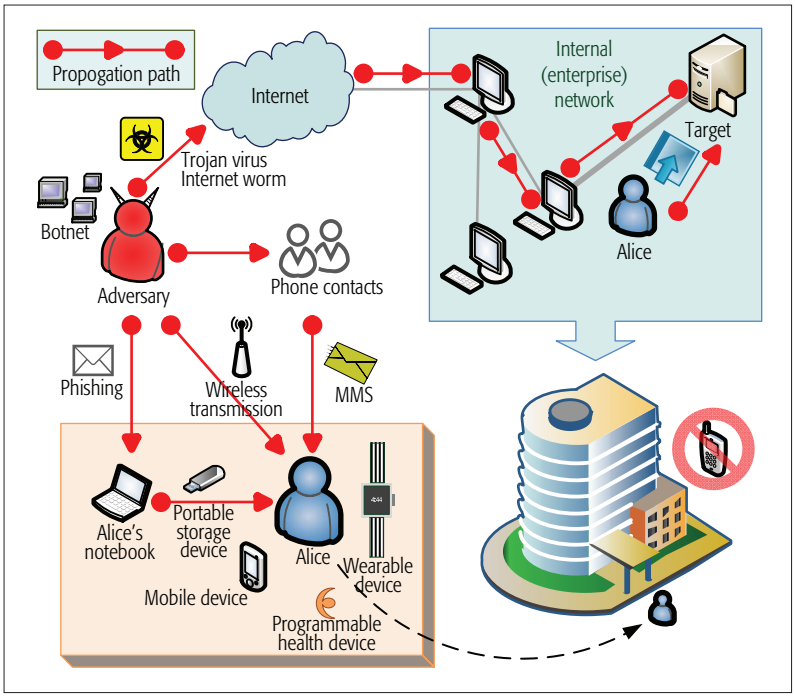

Figure 1. Illustration of transmissive attacks and their propagation paths. Transmissive attacks exploit various communication resources for propagation in order to reach the target. This diagram shows some examples of propagation paths that lead to the target.

devices, or health devices embedded in a human body equipped with communication capabilities. In practice, all the adversary needs to do to launch a transmissive attack is simply release a malicious code (e.g., a Trojan virus), and then sit back and wait for the code to propagate among hosts (potential victims), via either cyber connection (e.g., phishing from the Internet) or human carrier (e.g., Bluetooth or WiFi direct reception from proximity), to create an indirect (i.e., multihop) communication path for accessing the target. Moreover, after successful intrusion the adversary can erase its traces from the communication path (e.g., implementing a global timer for self-deactivation) to reduce the risk of being uncovered.

Inspired by biology, we use epidemic models to evaluate the consequences of a transmissive attack from a macroscopic system-level perspective. Analogous to disease transmission assessment, epidemic models categorize the hosts in a system into a few states to analyze the collective behavior of a system with parametric mathematical models (e.g., coupled state difference equations or Markov chains) for the purposes of status tracking, outbreak prediction, and further actions. As a first step toward analyzing transmissive attacks, we use epidemic models to investigate the probability of successfully compromising the target and quantify the risk of exposure with respect to time. We show that the trade-offs in time between the probability of successful intrusion to the target and the associated risk can be characterized by epidemic models, thereby enabling security analysis.[2]

Transmissive Attacks in Practice

As illustrated in Fig. 1, one typical scenario of transmissive attack is that an adversary aims to approach a target by propagating through intermediate hosts via all possible communication resources in a complex communication system. The purpose of such indirect propagation can be that direct access from the adversary to the target is unavailable, or the adversary attempts to hide his/her true identity by manipulating compromised machines to launch an attack, such as the exploitation of mobile devices as botnets [11]. It is worth noting that a transmissive attack can be more insidious due to inherent configurability of electronic devices carried by a user (e.g., programmable in-body health devices or wearable mobile devices), which enables malware propagation even when typical communication devices such as cell phones and laptops are prohibited.

In addition to hidden identity, another appealing advantage of the transmissive attack is that the adversary need not know the complete network topology to accomplish the attack. All the adversary needs to do is release a transmissive malicious code and then wait for the malicious code to propagate to the target due to its transmissive nature. In practice a transmissive attack can be accomplished simply by devising a Trojan virus designed to be operated in the stealthy transmissive mode during propagation and activated when reaching the target. Advanced transmissive attacks can camouflage normal user/network activities to elude intrusion detection or system monitoring, thereby incurring severe threats to security and privacy.

One of the most notable targeted attacks is the Stuxnet attack discovered in 2010. Stuxnet is designed to target a specific version of industrial control systems in a surreptitious manner, whereas traditional worms often aim to infest as many hosts as possible in a short time period. Stuxnet thus exhibits several distinguishing characteristics compared to traditional worms: each Stuxnet worm only replicates itself for at most three times; it is programmed to self-destruct on a day in 2012; it can stealthy propagate via carriers (i.e., vulnerable Windows computers) without showing any symptoms, and only unpack its malicious payload when reaching a target; multiple zero-day vulnerabilities are used. Although performing a targeted attack may be expensive, and indeed Stuxnet is believed to be state-sponsored malware due to its unprecedented level of sophistication, more and more Stuxnet successors (e.g., dudu and Flame) demonstrate how far an adversary is willing to go for high-value targets.

Stuxnet is one kind of advanced persistent threat (APT), which can be seen as one specific case of transmissive attack. An APT possesses the feature of specificity in targets. Although the feature of heterogeneity in community paths is not mandatory for an APT, it would shorten the process to approach the targets if heterogeneous community paths are considered. In 2013, Mandiant[3] summarized the attack life cycle of APT:

1. Initial compromise
2. Establish foothold
3. Escalate privileges
4. Internal reconnaissance
5. Move laterally
6. Maintain presence
7. Complete mission

[2] Although in recent years epidemic-like information propagation has been well studied in the communications society in the context of "epidemic routing," where packets are transmitted in a store-and-forward fashion in intermittently connected networks, little is known on how to apply these well developed analysis tools [7–10] to model transmissive attacks and beyond.

[3] APT1: Exposing One of China's Cyber Espionage Units, http://intelreport.mandiant.com/}

Application platforms	Number of vulnerabilities		
	2013	2014	2015
Adobe Acrobat Reader	66	44	129
Apple iPhone OS	90	120	375
Apple Mac OS X	65	135	384
Apple WatchOS	–	–	53
Google Android	7	11	130
Microsoft Internet Explorer	129	243	231
Microsoft Office	17	10	40
Microsoft Windows 7	100	36	147
Linux Kernel	189	133	77

Table 1. Statistics of vulnerabilities identified on popular applications and platforms.

An APT attack often loops through steps 3 to 6 until it reaches the specific target. These steps are also applicable to transmissive attacks.

To launch a successful transmissive attack, an attacker would also like to increase heterogeneity in community paths (e.g., by exploiting diverse vulnerabilities). The statistics of recently reported vulnerabilities (Table 1) shows the numbers are consistently increasing for most platforms and applications, even for modern mobile and wearable devices. Consequently, various activities and media, including web downloads, document reading, e-mail reading, short messages delivery, Wi-Fi access, Bluetooth access, and NFC contacts, can be used together to deliver malicious payloads and approach targets. By leveraging these existing vulnerabilities, an attacker can even launch transmissive attacks in the background and be invisible to a user.

For example, in July 2015, an unprecedented vulnerability in the Android system called Stagefright was revealed by the cyber security firm Zimperium.[4] Stagefright leverages the vulnerability of the media library to access users' Android devices through a simple multimedia message service (MMS) without users' awareness.[5,6,7] As approximately 80 percent of mobile devices use Android systems, nearly 1 billion devices are potential victims.[3,4,5] By viewing mobile users using different operating systems as hosts with different levels of immunity to a virus, the Stagefright vulnerability behaves like host specificity in epidemiology, as it can compromise users using Android systems.

Overview of Epidemic Models

Here we provide an overview of classical epidemic models that have been applied to communication systems, particularly for modeling information dissemination, malware propagation, and developing the associated control methods.[8]

Following terminologies from biology and epidemiology, each device in a communication system can be categorized into a few states representing its status. The main utility of such an abstraction is that one can leverage epidemic models to simplify complicated interactions among individuals and extract collective information for large-scale analysis and prediction, for example, tracking pandemic spread patterns and predicting their outbreaks in terms of the infected population. A popular analogy is that each device is either in the *susceptible* (S), *infected* (I), or *recovered* (R) state, known as the SIR model.

For epidemic modeling of normal information dissemination dynamics, including routing in communication networks, rumor, news spread in social networks, and so on, an infected individual means he/she carries a certain message (e.g., a data packet) to be delivered, a susceptible individual means he/she does not carry that message but can potentially be infected, and a recovered individual means he/she is immune to the message and hence ignores the message upon reception; for example, in a cooperative relay-assisted network a device in the recovered state will refuse to receive or forward the packet.

For epidemic modeling of malicious codes propagation dynamics, such as privilege escalation or system vulnerability leakage, an infected individual means he/she is compromised by a malicious code and is being leveraged as a warm bed for further propagation or attack (e.g., a botnet). A susceptible individual means he/she is not compromised, but is still vulnerable to the malicious code. A recovered individual means he/she is free of the threats incurred from the malicious code (e.g., securing one's devices via frequent security patch updates).

The following paragraphs introduce three basic epidemic models and relevant control techniques.

SI Model

The SI model assumes each individual is either in the susceptible or infected state. It can be used to estimate the reception performance of a broadcasting protocol or the dynamics of a malicious code. In [4], the authors show that information dissemination in a fully mixed network of dynamic topology and opportunistic links, such as a mobile contact-based network that possesses time-varying traces due to mobility and temporal connections due to opportunistic contacts, can be captured by an SI model. In [12], the authors show that the trends of self-propagating Internet worms such as Code Red and Slammer can be successfully predicted by SI models. In [5], the authors use the SI model to formulate malware propagation in a hybrid network composed of a social network and a proximal network, where malware can leverage delocalized links (e.g., through MMS) and localized links (e.g., through Bluetooth) for propagation.

SIS Model

Similar to the SI model, the SIS model also assumes that each individual is in either the susceptible or the infected state. The difference is that an SIS model allows an individual to transition from the infected state to the susceptible state. SIS models can be well mapped to the formulation of a typical two-state Markov chain where the steady-state behavior of the entire system is used for analysis. The utility of SIS models can be found in formulating recurrent network

SIS models can be well mapped to the formulation of a typical two-state Markov chain where the steady-state behavior of the entire system is used for analysis. The utility of SIS models can be found in formulating recurrent network behaviors, such as the trends of receiving spam mails, or information dissemination in an evolving environment with system reconfiguration factors.

[4] https://www.zimperium.com/

[5] http://fortune.com/2015/07/27/stagefright-android-vulnerability-text/

[6] http://www.forbes.com/sites/thomasbrewster/2015/07/27/android-text-attacks/

[7] As quoted from Zimperium chief technology officer Zuk Avraham, "These vulnerabilities are extremely dangerous because they do not require that the victim take any action to be exploited. Unlike spear-phishing, where the victim needs to open a PDF file or a link sent by the attacker, this vulnerability can be triggered while you sleep. Before you wake up, the attacker will remove any signs of the device being compromised and you will continue your day as usual – with a trojaned phone." Source: http://venturebeat.com/2015/07/27/researchers-find-vulnerability-that-affects-95-of-android-devices

[8] Due to reference count limitations only a subset of related works are introduced in this section. Interested readers can refer to [7–10, references therein] for more details.

Although transmissive attacks can be a serious threat to cyber security, they are often accompanied by an additional price compared to traditional attack schemes. Notably, their spreading nature and self-propagating patterns enhance the risk of exposure, and hence the attacks may be more likely to be detected.

behaviors, such as the trends of receiving spam mails, or information dissemination in an evolving environment with system reconfiguration factors. In [13], the authors integrate the SIS model with queueing theory to study malware propagation dynamics in a dynamic network.

SIR Model

The SIR model is a widely used model in energy-constrained systems (e.g., a wireless sensor network) or communication systems with control capabilities over information delivery (e.g., a configurable routing protocol). An infected individual can transition from the infected state to the recovered state when certain events occur; for example, a sensor stops forwarding packets due to battery drain. A susceptible node can transition to the recovered state when certain mechanisms are activated; for example, a computer is no longer vulnerable to a malicious code after installing the corresponding security patch or upgrading its operating system. In [14], the SIR model is used to study the vulnerability of broadcast protocols in wireless sensor networks. In [7, 8], the SIR model is used to analyze the performance of several protocols for epidemic routing.

Control Techniques

One major advantage of using epidemic models for modeling dynamics of information delivery or malware propagation lies in the fact that their analytical expressions closely resemble coupled state equations appearing in control theory, which allows one to quantify a cost function of interest and evaluate the performance of a control strategy. A commonly used cost function rooted in various applications is the accumulated infected population within a time interval. For instance, in store-and-forward routing schemes such as epidemic routing, the accumulated infected population from the time when a source releases a packet to the time when the packet is no longer carried by any individual is considered as a cost function for data transmission. It can be interpreted as the system-wise buffer occupancy for data transmission since all infected devices need to keep the packet in their own buffer until the destination successfully receives the packet.

Notably, although epidemic routing enables communications in intermittently connected networks, its spreading nature inevitably induces additional system burden, especially for buffer occupancy. In [7], the authors propose two strategies for controlling buffer occupancy, which we call the *global timeout scheme* and the *antipacket dissemination scheme*. In the global timeout scheme, each infected individual drops the packet in its buffer when the global timer expires. In the antipacket dissemination scheme, as motivated by vaccination from immunology, upon packet reception the destination releases an antipacket as an indicator of acknowledgment (ACK) and asks every encountered individual to forward the antipacket so that infected nodes can erase the obsolete packet from its buffer, and susceptible nodes can be prevented from receiving the already delivered packet, and hence achieve buffer occupancy reduction.

In [9], the authors consider time-dependent control capability of SIR models in hybrid networks, where the control ability is proportional to the elapsed time; that is, the ability to restrain malware propagation increases with the time spent in reverse-engineering its operations. An optimal control strategy based on dynamic programming is proposed for solving the optimal time to implement the control strategy (analogously releasing the antidotes) in order to balance the trade-offs between effectiveness and consequences.

Connecting the Dots: Evaluating Transmissive Attacks via Epidemic Models

Although transmissive attacks can be a serious threat to cyber security, they are often accompanied by an additional price compared to traditional attack schemes. Notably, their spreading nature and self-propagating patterns enhance the risk of exposure, and hence the attacks may be more likely to be detected. Generally speaking, while an attacker can accelerate the processes of reaching the target by compromising additional hosts, such an increased level of malicious activities becomes easily identified, thereby jeopardizing the purpose of the attack. To this end, there is a trade-off between the probability of a successful attack and the risk of being detected due to excessive exposure.

To quantify this trade-off between attack success and risk of exposure for transmissive attacks, we propose to use epidemic models for analysis. The risk of exposure is the accumulated infected population (i.e., accumulated number of compromised hosts) from time 0 when the adversary launches a transmissive attack to time T when the target is comprised, or the time when the adversary decides to abort the attack, as the longer the duration of a host being compromised renders an attack more prone to detection. The attack success at a time instance t is defined as the probability of successfully accessing the target between time intervals 0 and t.

For further illustration, we consider the scenario where the adversary adopts the global timeout scheme for transmissive attacks as his/her control technique to reduce the risk of exposure. A global timer is set since the attacker launches a transmissive attack, and upon global timer expiration all malware residing in the compromised hosts will erase their traces via complete self-deletion, whether the attack is successful or not, so as to allow the adversary to constrain malware propagation and alleviate exposure.

Under the global timeout scheme, an interesting question that naturally arises is: what is the optimal global timeout value T_G such that the attack success at time T_G is no less than a certain value (e.g., 80 percent) while the risk of exposure can be minimized? Partial answers to this question have been given in the contexts of minimizing the system buffer occupancy while simultaneously guaranteeing end-to-end data delivery reliability between a source-destination pair for epidemic routing [15], where the data delivery reliability and buffer occupancy are proven to be associated with the accumulated infected population under the SIR model [8].

In particular, if the mobility pattern follows a

homogeneous mixing mobility assumption, such as the random waypoint model or the random direction model, a closed-form expression of optimal global timeout value is provided in [15] in which, given a data delivery reliability guarantee, the optimal global timeout value that minimizes the system buffer occupancy depends on the initially infected population and the pairwise meeting rate. This suggests that if mobile botnets (i.e., several initially compromised hosts) are utilized to launch a transmissive attack, the global timer should be set smaller than that of a single seed to minimize the risk of exposure. Similarly, the global timer should decrease when the pairwise meeting rate is higher due to more frequent encounters facilitating malware propagation. Moreover, an interesting finding in [15] is that the optimal buffer occupancy grows exponentially with the data delivery reliability. Analogously, for transmissive attacks the exponential growth rate suggests that the risk of exposure can be significantly amplified if an adversary desires higher attack success.

It is also proven in [15] that when adopting the optimal global timer, the per-user buffer occupancy does not depend on the total population for epidemic routing. This suggests that for transmissive attacks, the risk of exposure for a single host can be controlled to a certain extent such that its local risk does not increase with the total host number.

Experiments and Simulations

In this section we conduct several simulations and experiments as a first step toward the analysis of transmissive attacks using epidemic models. In particular, we investigate the trade-offs between the attack success and risk of exposure by simulating global-timeout-value-enabled transmissive attacks in mobile networks with two widely adopted mobility models: the random waypoint (RWP) mobility model and the random direction (RD) mobility model. We also evaluate the effect of propagation path diversity of a mobile social network on transmissive attacks based on mobile and social interaction patterns extracted from real-life datasets.

Simulation of Transmissive Attacks in Mobile Networks

We simulate the traces of a mobile network of N mobile users moving around in a wrap-around $L \times L$ square area. Any pair of users can exchange information for communication when they are within distance r of each other. For the RWP mobility model each user selects a destination at random and travels to the destination at a constant speed v. Similarly, for the RD mobility model each user selects a direction at random and travels at a constant speed v. For both models the speed v is randomly and uniformly drawn from the interval $[v_{\min}, v_{\max}]$. Initially (at time 0), one user is compromised to launch a transmissive attack, and the target is selected at random.

Figures 2 and 3 display the attack success and the risk of exposure with respect to the global timeout value T_G, respectively. Given T_G, the attack success is defined as the fraction of simulated transmissive attacks that successfully approach the target prior to time T_G among all trials, and the risk of exposure is defined as the accumulated compromised population divided by the total population N. The SIR epidemic model proposed in [15] is used for performance comparison. The successful rate is the probability of infecting a particular host, and the risk of exposure is evaluated using the accumulated infected population.

It can be observed that the global timeout value T_G indeed governs the performance of both attack success and risk of exposure. The simulation results also validate the trade-offs between these two metrics as the enhancement of attack vulnerability often leads to an increased

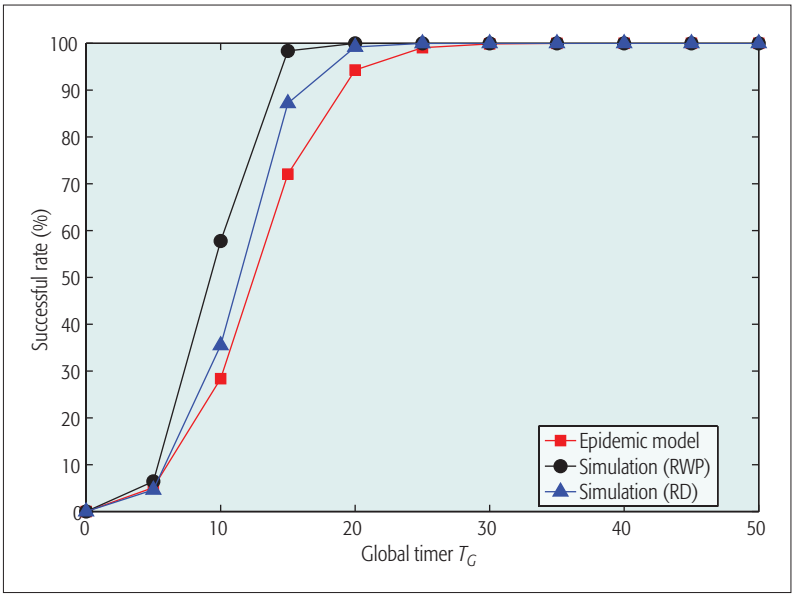

Figure 2. Successful rate for transmissive attacks with respect to varying global timeout value T_G in mobile networks simulated by RD and RWP mobility models. The system parameters are $N = 100$ mobile users, $r = 0.1$ km, $L = 2.5352$ km, $v_{\min} = 4$ km/h, $v_{\max} = 10$ km/h, and pairwise meeting rate = 0.37043. The results are averaged over 10,000 trials.

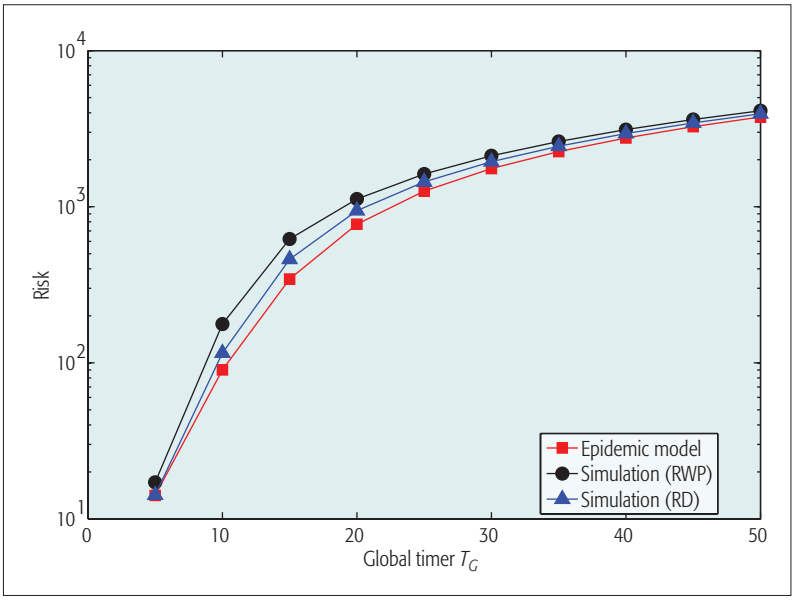

Figure 3. Risk metric corresponding to Fig. 2. Epidemic models are capable of predicting both the attack success and risk of exposure.

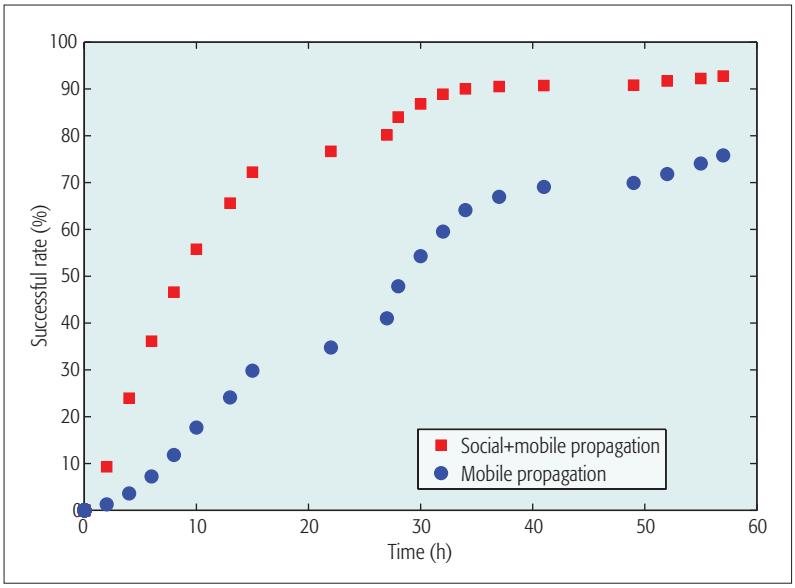

Figure 4. Successful rate for transmissive attacks in a mobile social network: exploiting both social and mobile propagation paths can significantly improve the possibility of approaching the target. The propagation parameters $p_s = p_\ell = 0.05$, and the results are averaged over 10,000 trials.

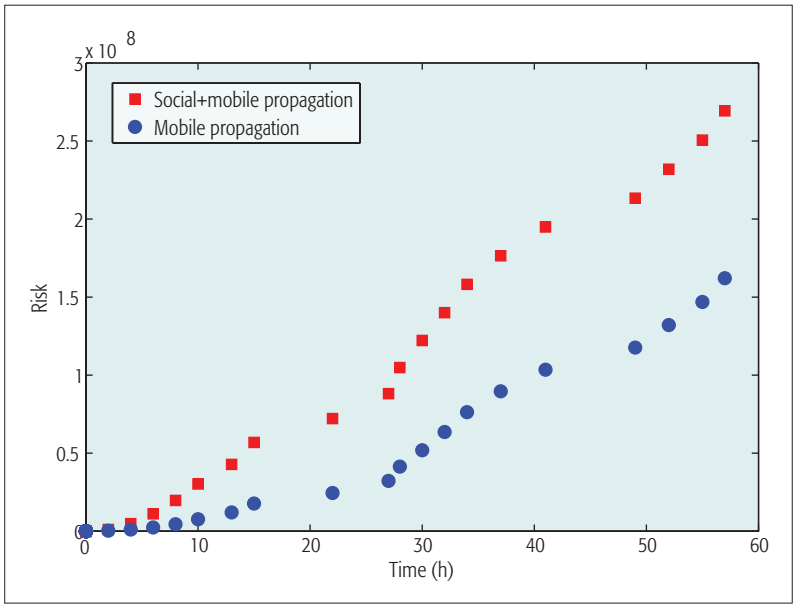

Figure 5. Risk metric corresponding to Fig. 4: the accumulated infected population with respect to time. The results show clear trade-offs between attack success and risk of exposure.

risk of exposure, and vice versa. For example, to enhance the attack success from 30 percent ($T_G = 10$) to 90 percent ($T_G = 20$), the risk of exposure needs to be amplified 10 times. Notably, the predicted results from the epidemic model can successfully capture the trends of these two metrics. An immediate utility is that an adversary can use the epidemic model to determine the optimal global timeout value that guarantees the attack success while simultaneously minimizing the risk of exposure (e.g., selecting $T_G = 25$ such that the attack success is no less than 95 percent). Moreover, a defender can also utilize the epidemic model to evaluate a system's vulnerability without conducting time-consuming simulations.

[9] CRAWDAD dataset thlab/sigcomm2009 (v. 2012-07-15); http://crawdad.org/thlab/sigcomm2009/20120715

Experiment of Transmissive Attacks in Mobile Social Networks

To investigate the impact of propagation path diversity on transmissive attacks, we use the CRAWDAD mobile-social interaction traces[9] to simulate a transmissive attack. The purpose of this experiment is to study the consequences of transmissive attacks that are capable of propagating through social contacts (e.g., via MMS) or proximity contacts (e.g., via Bluetooth). In such a mobile social network the malware can propagate from one compromised user to another user with probability of success p_s via the social propagation path if these two users are social contacts (i.e., there is an edge between these two users in the corresponding social graph). Similarly, the malware can propagate from one compromised user to another user with probability of success p_ℓ via the proximity propagation path if these two users are within a physical contact distance.

Figures 4 and 5 display the attack success and risk of exposure for transmissive attacks in the mobile social network, respectively. It can be observed that the inclusion of social propagation paths can significantly enhance the attack success. For example, after 30 hours since launching a transmissive attack, the attack success in utilizing both social and mobile propagation paths can be doubled compared to the attack success of only exploiting mobile propagation paths. However, the induced risk metric is also amplified, as shown in Fig. 5.

Additional experiments of different parameter configurations show similar trends in attack success and risk of exposure, which are discussed in the supplementary file.[1] These results suggest that propagation path diversity can facilitate transmissive attacks at the price of potentially amplified exposure. In addition, how current epidemic models can be improved to model transmissive attacks in such a heterogeneous network is an active research area.

Some Ongoing Challenges and Open Research Questions

Here we discuss several ongoing challenges and open research questions related to transmissive attacks.

Lateral movement detection and prevention: Unlike disruption attacks (e.g., denial of service), which often cause distinguishable anomalous activities, lateral movement attacks (e.g., privilege escalation that insidiously acquires user credentials) are difficult to detect. Transmissive attacks fall into one category of lateral movement attacks due to their stealthy transmissive nature. If detecting lateral movement is implausible, one may shift attention to designing a resilient cyber system that can constrain the damage induced by such attacks.

Transmissive attacks in a network of networks: A network of networks (NoNs) is an intuitive explanation of modern communication systems with intrinsic layered structures and heterogeneous networks. The layers of the Internet architecture can be operated by different protocols, and a device can have multiple communication resources (e.g., cellular, WiFi, and Bluetooth modules).

As horizontal malware propagations within a single layer/system can be straightforward by lever-

aging similar vulnerabilities, vertical malware propagations traversing different layers/systems can be more difficult due to lack of common vulnerabilities or implementation of additional security rules. In terms of bio-inspired attacks, transmissive attacks that are self-evolving and adaptive to the NoN environment can be a vital threat.

Data-driven inference for attack and defense: In a data-rich era, our cyber footage is everywhere and easy to track. Both attackers and defenders should make use of available data collected from different sources to infer vulnerabilities in a system. Notably, modern technology enables an adversary to optimize his/her attack strategy based on the inference results from collected data prior to launching a transmissive attack, known as the inference attacks. For instance, personal trace information such as GPS signals or locations revealed by online social networking activities can be directly observed or indirectly inferred from user-centric data.

Evolutionary resilience of dynamic systems: In many cases the underlying communication system where a transmissive attack takes place is an ever changing system due to variations in time, traffic flows, evolution of communication technology, and so on. Therefore, a general notion of resilience for such a dynamic system is necessary to quantify network stability that can vary with time, which we call *evolutionary resilience*. Notably, biology models such as ecological systems, predator-prey models, and evolutionary game theory that target evolutionary stability in time-varying coupled systems may be well mapped to analyze transmissive attacks in dynamic systems.

Conclusion

This article introduces an emerging attack pattern called transmissive attack that leverages diverse communication paths to approach a target and accomplish its task. Inspired by biology, we provide an overview of commonly used epidemic models for communication systems, and connect the dots between transmissive attacks and epidemic models. We perform simulations via two widely used mobility models and conduct experiments in mobile social networks to demonstrate the utility of epidemic models for assessing attack success and risk of exposure, and we also discuss some ongoing research challenges and open research questions related to transmissive attacks.

Acknowledgment

This work was supported in part by Taiwan Information Security Center (TWISC), Academia Sinica, and Ministry of Science and Technology, Taiwan, under the grant MOST 103-2221-E-009-230-MY2, 104-2218-E-001-002, 104-2923-E-011-006-MY2, and 104-2221-E-009-200-MY3. The first author would like to thank Mr. Ming-Yann Lee (M.D.) at the Department of Medical Imagine, National Taiwan University Hospital, for his help in clarifying terminologies in biology and epidemiology.

References

[1] W. Mazurczyk and E. Rzeszutko, "Security – A Perpetual War: Lessons from Nature," *IEEE IT Professional*, vol. 17, no. 1, Jan. 2015, pp. 16–22.
[2] S.-M. Cheng and P.-Y. Chen, "Ecology-Based DoS Attack in Cognitive Radio Networks," 2016, arXiv:1603.01315.
[3] P. Wang *et al.*, "Understanding the Spreading Patterns of Mobile Phone Viruses," *Science*, vol. 324, May 2009, pp. 1071–75.
[4] P.-Y. Chen and K.-C. Chen, "Information Epidemics in Complex Networks with Opportunistic Links and Dynamic Topology," *Proc. IEEE GLOBECOM*, Dec. 2010.
[5] S.-M. Cheng *et al.*, "On Modeling Malware Propagation in Generalized Social Networks," *IEEE Commun. Lett.*, vol. 15, no. 1, Jan. 2011, pp. 25–27.
[6] S.-M. Cheng *et al.*, "Diffusion Models for Information Dissemination Dynamics in Wireless Complex Communication Networks," *J. Complex Systems*, 2013.
[7] Z. J. Haas and T. Small, "A New Networking Model for Biological Applications of Ad Hoc Sensor Networks," *IEEE/ACM Trans. Net.*, vol. 14, no. 1, Feb. 2006, pp. 27–40.
[8] X. Zhang *et al.*, "Performance Modeling of Epidemic Routing," *Comp. Net.*, vol. 51, no. 8, July 2007, pp. 2867–91.
[9] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen, "Optimal Control of Epidemic Information Dissemination Over Networks," *IEEE Trans. Cybernetics*, vol. 44, no. 12, Dec. 2014, pp. 2316–28.
[10] S. Peng, S. Yu, and A. Yang, "Smartphone Malware and Its Propagation Modeling: A Survey," *IEEE Commun. Surveys & Tutorials*, vol. 16, no. 2, 2014, pp. 925–41.
[11] A. Mtibaa, K. Harras, and H. Alnuweiri, "From Botnets to Mobibots: A Novel Malicious Communication Paradigm for Mobile Botnets," *IEEE Commun. Mag.*, vol. 53, no. 8, Aug. 2015, pp. 61–67.
[12] C. C. Zou *et al.*, "The Monitoring and Early Detection of Internet Worm," *IEEE/ACM Trans. Net.*, vol. 13, no. 5, Oct. 2005, pp. 961–74.
[13] V. Karyotis and S. Papavassiliou, "Macroscopic Malware Propagation Dynamics for Complex Networks with Churn," *IEEE Commun. Lett.*, vol. 19, no. 4, Apr. 2015, pp. 577–80.
[14] P. De, Y. Liu, and S. Das, "An Epidemic Theoretic Framework for Vulnerability Analysis of Broadcast Protocols in Wireless Sensor Networks," *IEEE Trans. Mobile Comp.*, vol. 8, no. 3, Mar. 2009 , pp. 413–25.
[15] P.-Y. Chen, M.-H. Sung, and S.-M. Cheng, "Buffer Occupancy and Delivery Reliability Tradeoffs for Epidemic Routing," 2016, arXiv:1601.06345.

Biographies

Pin-Yu Chen [S'10] (pinyu@umich.edu) received his B.S. degree in electrical engineering and computer science (undergraduate honors program) from National Chiao Tung University, Taiwan, in 2009, and his M.S. degree in communication engineering from National Taiwan University in 2011. He is currently working toward his Ph.D. degree in electrical engineering and computer science at the University of Michigan, Ann Arbor. His research interests include network science, interdisciplinary network analysis, graph clustering and community detection, statistical graph signal processing, cyber security, and their applications to data analysis and communication systems. He is a member of the Tau Beta Pi Honor Society and the Phi Kappa Phi Honor Society, and was the recipient of the Chia-Lun Lo Fellowship. He was also the recipient of the IEEE GLOBECOM 2010 GOLD Best Paper Award, an IEEE ICASSP 2014 NSF travel grant, and an IEEE ICASSP 2015 SPS travel grant.

Ching-Chao Lin (m10415008@mail.ntust.edu.tw) received his B.S. degree in computer science and information engineering from National Taiwan University of Science and Technology, Taipei, in 2015. He is currently working toward his M.S. degree in computer science and information engineering at National Taiwan University of Science and Technology. His research interests include cyber security and wireless networks.

Shin-Ming Cheng [S'05, M'07] (smcheng@mail.ntust.edu.tw) received his B.S. and Ph.D. degrees in computer science and information engineering from National Taiwan University in 2000 and 2007, respectively. He was a postdoctoral research fellow at the Graduate Institute of Communication Engineering, National Taiwan University, from 2007 to 2012. Since 2012, he has been with the Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology as an assistant professor. His current research interests include mobile networks, wireless communication, cyber security, and complex networks. He was a recipient of the IEEE PIMRC 2013 Best Paper Award and the 2014 ACM Taipei/Taiwan Chapter K. T. Li Young Researcher Award.

Hsu-Chun Hsiao (hchsiao@csie.ntu.edu.tw) is an assistant professor in the Department of Computer Science and Information Engineering and Graduate Institute of Networking and Multimedia at National Taiwan University. She also holds an adjunct assistant researcher position at Academia Sinica. She completed her B.S. (2006) and M.S. (2008) in electrical engineering at National Taiwan University, and her Ph.D. at Carnegie Mellon University (2014). Her research interests include network security, anonymity and privacy, and applied cryptography.

Chun-Ying Huang [S'03, M'08] (chuang@cs.nctu.edu.tw) is an associate professor in the Department of Computer Science, National Chiao Tung University. He leads the security and systems laboratory at National Chiao Tung University. From 2008 to 2013, he was an assistant professor in the Department of Computer Science and Engineering, National Taiwan Ocean University, and was an associate professor in the same deparment from 2013 to 2016. He received his Ph.D in electrical engineering from National Taiwan University in 2007. His research interests include system security, multimedia networking, and mobile computing. He is a member of ACM and IEEE. He was a recipient of the 2014 ACM Taipei/Taiwan Chapter K. T. Li Young Researcher Award.

In many cases the underlying communication system where a transmissive attack takes place is an ever-changing system due to variations in time, traffic flows, evolution of communication technology, and so on. Therefore, a general notion of resilience for such a dynamic system is necessary to quantify network stability that can vary with time, which we call evolutionary resilience.