Identifying Passive Message Fingerprint Attacks via Honey Challenge in Collaborative Intrusion Detection Networks

To enhance the detection capability of a single intrusion detection system (IDS), collaborative intrusion detection networks (CIDNs) have been exploited and developed via enabling a set of IDS nodes to exchange information with each other. In CIDNs, challenge-based trust mechanism has been considered as one promising solution to identify malicious nodes by evaluating the satisfaction levels between challenges and responses. However, such mechanism is still vulnerable to some advanced insider attacks like passive message fingerprint attack (PMFA), which is deemed as an advanced attack on challenge-based CIDNs by collecting messages and identifying normal requests in a passive way. In this work, we focus on PMFA and design Honey Challenge, an improved challenge mechanism for challenge-based CIDNs characterized by sending challenges in a similar way of sending normal requests, in such a way malicious nodes cannot accurately identify the normal requests. In the evaluation, we investigate the attack performance under both simulated and real network environments. Experimental results demonstrate that our proposed mechanism can identify malicious nodes under PMFA and decrease their trust values in a quick manner.

A fog-based privacy-preserving approach for distributed signature-based intrusion detection

Intrusion detection systems (IDSs) are the frontier of defense against transmissible cyber threats that spread across distributed systems. Modern IDSs overcome the limitation of hardware processing power by offloading computation extensive operations such as signature matching to the cloud. Moreover, in order to prevent the rapid spread of transmissible cyber threats, collaborative intrusion detection schemes are widely deployed to allow distributed IDS nodes to exchange information with each other. However, no party wants to disclose their own data during the detection process, especially sensitive user data to others, even the cloud providers for privacy concerns. In this background, privacy-preserving technology has been researched in the field of intrusion detection, whereas a collaborative intrusion detection network (CIDN) environment still lacks of appropriate solutions due to its geographical distribution. With the advent of fog computing, in this paper, we propose a privacy-preserving framework for signature-based intrusion detection in a distributed network based on fog devices. The results in both simulated and real environments demonstrate that our proposed framework can help reserve the privacy of shared data, reduce the workload on the cloud side, and offer less
detection delay as compared to similar approaches.

**General information**
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Guangzhou University, City University of Hong Kong, Swinburne University of Technology
Contributors: Wang, Y., Meng, W., Li, W., Li, J., Liu, W., Xiang, Y.
Pages: 26-35
Publication date: 2018
Peer-reviewed: Yes

**Publication information**
Journal: Journal of Parallel and Distributed Computing
Volume: 122
ISSN (Print): 0743-7315
Ratings:
BFI (2018): BFI-level 2
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 2
Scopus rating (2017): CiteScore 2.91 SJR 0.502 SNIP 1.674
Web of Science (2017): Impact factor 1.815
Web of Science (2017): Indexed yes
BFI (2016): BFI-level 2
Scopus rating (2016): CiteScore 2.6 SJR 0.597 SNIP 1.809
Web of Science (2016): Impact factor 1.93
BFI (2015): BFI-level 2
Scopus rating (2015): CiteScore 2.16 SJR 0.614 SNIP 1.507
Web of Science (2015): Impact factor 1.32
BFI (2014): BFI-level 2
Scopus rating (2014): CiteScore 2.18 SJR 0.548 SNIP 1.88
Web of Science (2014): Impact factor 1.179
BFI (2013): BFI-level 2
Scopus rating (2013): CiteScore 2.07 SJR 0.437 SNIP 1.691
Web of Science (2013): Impact factor 1.011
ISI indexed (2013): ISI indexed yes
BFI (2012): BFI-level 2
Scopus rating (2012): CiteScore 1.83 SJR 0.397 SNIP 1.604
ISI indexed (2012): ISI indexed yes
BFI (2011): BFI-level 2
Scopus rating (2011): CiteScore 2.18 SJR 0.485 SNIP 2.019
Web of Science (2011): Impact factor 0.859
ISI indexed (2011): ISI indexed yes
BFI (2010): BFI-level 2
Scopus rating (2010): SJR 0.509 SNIP 1.523
Web of Science (2010): Impact factor 1.078
BFI (2009): BFI-level 2
Scopus rating (2009): SJR 0.489 SNIP 1.233
BFI (2008): BFI-level 2
Scopus rating (2008): SJR 0.586 SNIP 1.313
Scopus rating (2007): SJR 0.442 SNIP 1.166
Scopus rating (2006): SJR 0.49 SNIP 1.372
Scopus rating (2005): SJR 0.489 SNIP 1.709
Scopus rating (2004): SJR 0.499 SNIP 1.675
Scopus rating (2003): SJR 0.459 SNIP 1.177
Scopus rating (2002): SJR 0.304 SNIP 0.943
CyberShip: An SDN-based Autonomic Attack Mitigation Framework for Ship Systems

The use of Information and Communication Technology (ICT) in the ship communication network brings new security vulnerabilities and make communication links a potential target for various kinds of cyber physical attacks, which results in the degradation of the performance. Moreover, crew members are burdened with the task of configuring the network devices with low-level device specific syntax for mitigating the attacks. Heavy reliance on the crew members and additional software and hardware devices makes the mitigation difficult and time consuming process. Recently, the emergence of Software-Defined Networking (SDN) offers a solution to reduce the complexity in the network management tasks.

To explore the advantages of using SDN, we propose a framework based on SDN and a use case to mitigate the attacks in an automated way for improved resilience in the ship communication network.

Detecting insider attacks in medical cyber–physical networks based on behavioral profiling

Cyber–physical systems (CPS) have been widely used in medical domains to provide high-quality patient treatment in complex clinical scenarios. With more medical devices being connected in industry, the security of medical cyber–physical systems has received much attention. Medical smartphones are one of the widely adopted facilities in the healthcare industry aiming to improve the quality of service for both patients and healthcare personnel. These devices construct an emerging CPS network architecture, called medical smartphone networks (MSNs). Similar to other distributed networks, MSNs also suffer from insider attacks, where the intruders have authorized access to the network resources, resulting in the leakage of patient information. In this work, we focus on the detection of malicious devices in MSNs and design a trust-based intrusion detection approach based on behavioral profiling. A node’s reputation can be judged by identifying the difference in Euclidean distance between two behavioral profiles. In the evaluation, we evaluate our approach in a real MSN environment by collaborating with a practical healthcare center. Experimental results demonstrate that our approach can identify malicious MSN nodes faster than other similar approaches.
Original language: English
Keywords: Behavioral profiling, Collaborative network, Intrusion detection, Medical cyber-physical system, Trust management
DOIs:
10.1016/j.future.2018.06.007
Source: FindIt
Source-ID: 2435323090
Research output: Research - peer-review; Journal article – Annual report year: 2018
Editorial of special issue on mobile networks and devices security, privacy and trust

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Nanjing University of Aeronautics and Astronautics, University of Salerno, Hong Kong Polytechnic University
Contributors: Meng, W., Liu, Z., Castiglione, A., Au, M. H.
Pages: 170-171
Publication date: 2018
Peer-reviewed: Yes

Publication information
Journal: Journal of Information Security and Applications
Volume: 41
ISSN (Print): 2214-2126
Ratings:
BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 1
Scopus rating (2017): CiteScore 2.27 SJR 0.346 SNIP 1.357
Web of Science (2017): Indexed yes
BFI (2016): BFI-level 1
Scopus rating (2016): CiteScore 1.65 SJR 0.375 SNIP 1.287
BFI (2015): BFI-level 1
Scopus rating (2015): SJR 0.338 SNIP 0.727
BFI (2014): BFI-level 1
Scopus rating (2014): SJR 0.198 SNIP 0.795
BFI (2013): BFI-level 1
Scopus rating (2013): SJR 0.168 SNIP 0.785
ISI indexed (2013): ISI indexed no
BFI (2012): BFI-level 1
Scopus rating (2012): SJR 0.242 SNIP 0.599
ISI indexed (2012): ISI indexed no
BFI (2011): BFI-level 1
Scopus rating (2011): SJR 0.209 SNIP 0.569
ISI indexed (2011): ISI indexed no
BFI (2010): BFI-level 1
Scopus rating (2010): SJR 0.277 SNIP 0.904
BFI (2009): BFI-level 1
Scopus rating (2009): SJR 0.165 SNIP 0.59
BFI (2008): BFI-level 1
Scopus rating (2008): SJR 0.177 SNIP 0.632
Scopus rating (2007): SJR 0.135 SNIP 0.286
Scopus rating (2006): SJR 0.165 SNIP 0.49
Scopus rating (2005): SJR 0.154 SNIP 0.562
Scopus rating (2004): SJR 0.131 SNIP 0.194
Scopus rating (2003): SJR 0.115 SNIP 0.14
Scopus rating (2002): SJR 0.111 SNIP 0.491
Scopus rating (2001): SJR 0.129 SNIP 0.181
Scopus rating (2000): SJR 0.083 SNIP 0.032
Scopus rating (1999): SJR 0.1 SNIP 0.343
Original language: English
DOIs:
10.1016/j.jisa.2018.07.006
Source: Findit
Source-ID: 2438176379
Research output: Research - peer-review » Editorial – Annual report year: 2018
Enhancing Intelligent Alarm Reduction for Distributed Intrusion Detection Systems via Edge Computing
To construct an intelligent alarm filter is a promising solution to help reduce false alarms for an intrusion detection system (IDS), in which an appropriate algorithm can be selected in an adaptive way. Taking the advantage of cloud computing, the process of algorithm selection can be offloaded to the cloud, but it may cause communication delay and additional burden on the cloud side. This issue may become worse when it comes to distributed intrusion detection systems (DIDSs), i.e., some IoT applications might require very short response time and most of the end nodes in IoT are energy constrained things. In this paper, with the advent of edge computing, we propose a framework for improving the intelligent false alarm reduction for DIDSs based on edge computing devices (i.e., the data can be processed at the edge for shorter response time and could be more energy efficient). The evaluation shows that the proposed framework can help reduce the workload for the central server and shorten the delay as compared to the similar studies.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Guangzhou University, Nanjing University of Aeronautics and Astronautics, The University of Hong Kong, UNITEC Institute of Technology
Contributors: Meng, W., Wang, Y., Li, W., Liu, Z., Li, J., Probst, C. W.
Pages: 759-767
Publication date: 2018

Host publication information
Title of host publication: Information Security and Privacy
Volume: 10946
Publisher: Springer
ISBN (Print): 9783319936376
(Lecture Notes in Computer Science, Vol. 10946).
Keywords: Intrusion detection, Intelligent false alarm filtration, Edge computing, Distributed environment, Cloud computing
DOI:
10.1007/978-3-319-93638-3_44
Source: FindIt
Source-ID: 2436372224
Research output: Research - peer-review » Article in proceedings – Annual report year: 2018

Evaluating the Impact of Juice Filming Charging Attack in Practical Environments
Nowadays, smartphones are widely adopted in people’s daily lives. With the increasing capability, phone charging has become a basic requirement and a large number of public charging facilities are under construction for this purpose. However, public charging stations may open a hole for cyber-criminals to launch various attacks, especially charging attacks, to steal phone user’s private information. Juice filming charging (JFC) attack is one such threat, which can refer users’ sensitive information from both Android OS and iOS devices, through automatically monitoring and recording phone screen during the whole charging period. Due to the potential damage of JFC attacks, there is a need to investigate its influence in practical scenarios. Motivated by this, in this work, we firstly conduct a large user survey with over 2500 participants about their awareness and attitude towards charging attacks. We then for the first time investigate the impact of JFC attack under three practical scenarios. Our work aims to complement the state-of-the-art and stimulate more research in this area.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Advanced Digital Sciences Center, Singapore, Singapore, Institute for Infocomm Research, University of Luxembourg, University of Aizu
Contributors: Meng, W., Lee, W., Liu, Z., Su, C., Li, Y.
Pages: 327-338
Publication date: 2018

Host publication information
Title of host publication: Information Security and Cryptology
Volume: 10779
Publisher: Springer
ISBN (Print): 9783319785554
Keywords: Computer Science, Systems and Data Security, Data Encryption, Artificial Intelligence (incl. Robotics), Smartphone privacy, Android and iOS, Video recording, Charging station, Juice filming charging attack, Practical evaluation
DOI:
10.1007/978-3-319-78556-1_18
Source: FindIt
Intrusion Detection in the Era of IoT: Building Trust via Traffic Filtering and Sampling

In the Internet of Things (IoT) era, the number of connected devices and subnets of devices is rapidly increasing. Yet, it remains a challenge for intrusion detection mechanisms to build a trust map among various IoT devices because of the devices’ large quantity and dynamic nature. Through a case study, the author highlights the importance of traffic filtration and sampling in evaluating trustworthiness among IoT devices.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security
Contributors: Meng, W.
Pages: 36-43
Publication date: 2018
Peer-reviewed: Yes

Publication information
Journal: Computer
Volume: 51
Issue number: 7
ISSN (Print): 0018-9162
Ratings:
BFI (2018): BFI-level 2
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 2
Scopus rating (2017): CiteScore 1.87 SJR 0.406 SNIP 1.798
Web of Science (2017): Impact factor 1.94
Web of Science (2017): Indexed yes
BFI (2016): BFI-level 2
Scopus rating (2016): CiteScore 1.82 SJR 0.423 SNIP 2.191
Web of Science (2016): Impact factor 1.755
BFI (2015): BFI-level 2
Scopus rating (2015): CiteScore 1.74 SJR 0.511 SNIP 2.662
Web of Science (2015): Impact factor 1.115
BFI (2014): BFI-level 2
Scopus rating (2014): CiteScore 1.91 SJR 0.542 SNIP 3.34
Web of Science (2014): Impact factor 1.443
BFI (2013): BFI-level 2
Scopus rating (2013): CiteScore 2.46 SJR 0.607 SNIP 4.347
Web of Science (2013): Impact factor 1.438
ISI indexed (2013): ISI indexed yes
BFI (2012): BFI-level 2
Scopus rating (2012): CiteScore 2.4 SJR 0.684 SNIP 5.31
Web of Science (2012): Impact factor 1.675
ISI indexed (2012): ISI indexed yes
BFI (2011): BFI-level 2
Scopus rating (2011): CiteScore 2.52 SJR 0.662 SNIP 4.826
Web of Science (2011): Impact factor 1.47
ISI indexed (2011): ISI indexed yes
BFI (2010): BFI-level 2
Scopus rating (2010): SJR 0.857 SNIP 5.339
Web of Science (2010): Impact factor 1.812
BFI (2009): BFI-level 2
Scopus rating (2009): SJR 0.745 SNIP 5.054
BFI (2008): BFI-level 2
Scopus rating (2008): SJR 0.854 SNIP 5.758
Investigating the influence of special on-off attacks on challenge-based collaborative intrusion detection networks

Intrusions are becoming more complicated with the recent development of adversarial techniques. To boost the detection accuracy of a separate intrusion detector, the collaborative intrusion detection network (CIDN) has thus been developed by allowing intrusion detection system (IDS) nodes to exchange data with each other. Insider attacks are a great threat for such types of collaborative networks, where an attacker has the authorized access within the network. In literature, a challenge-based trust mechanism is effective at identifying malicious nodes by sending challenges. However, such mechanisms are heavily dependent on two assumptions, which would cause CIDNs to be vulnerable to advanced insider attacks in practice. In this work, we investigate the influence of advanced on-off attacks on challenge-based CIDNs, which can respond truthfully to one IDS node but behave maliciously to another IDS node. To evaluate the attack performance, we have conducted two experiments under a simulated and a real CIDN environment. The obtained results demonstrate that our designed attack is able to compromise the robustness of challenge-based CIDNs in practice; that is, some malicious nodes can behave untruthfully without a timely detection.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, University of Hong Kong
Contributors: Li, W., Meng, W., Kwok, L. F.
Number of pages: 16
Publication date: 2018
Peer-reviewed: Yes

Publication information
Journal: Future Internet
Volume: 10
Issue number: 1
ISSN (Print): 1999-5903
Ratings:
Scopus rating (2017): CiteScore 1.25 SJR 0.219 SNIP 1.038
Web of Science (2017): Indexed yes
Scopus rating (2016): CiteScore 0.32 SJR 0.287 SNIP 1.801
Scopus rating (2015): SJR 0.604 SNIP 2.369
Scopus rating (2014): SJR 0.345 SNIP 1.556
Scopus rating (2013): SJR 0.318 SNIP 1.874
BFI (2012): BFI-level 1
Original language: English
Keywords: Collaborative network, On-off attack, Challenge-based Mechanism, Trust computation and management, Intrusion detectors
Electronic versions:
futureinternet_10_00006.pdf
DOIs:
10.3390/fi10010006
Source: FindIt
JFCGuard: Detecting juice filming charging attack via processor usage analysis on smartphones

Smartphones have become necessities in people's lives, so that many more public charging stations are under deployment worldwide to meet the increasing demand of phone charging (i.e., in airports, subways, shops, etc). However, this situation may expose a hole for cyber-criminals to launch various attacks especially charging attacks and threaten user's privacy. As an example, juice filming charging (JFC) attack is able to steal users' sensitive and private information from both Android OS and iOS devices, through automatically recording phone-screen and monitoring users' inputs during the whole charging period. More importantly, this attack does not need any permission or installing any pieces of apps on user's side. The rationale is that users' information can be leaked through a standard micro USB connector that employs the Mobile High-Definition Link (MHL) standard. Motivated by the potential damage of JFC attack, in this work, we investigate the impact of JFC attack on processor usage including both CPU- and GPU-usage. It is found that JFC attack would cause a noticeable usage increase when connecting the phone to the JFC charger. Then, we design a security mechanism, called JFCGuard, to detect JFC attack based on processor usage analysis for smartphone users. In the evaluation, we perform a user study with over 250 participants and the results demonstrate that JFCGuard can identify JFC attack in an effective way. Our work aims to complement existing research results and stimulate more research in this area.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Guangzhou University, Swinburne University of Technology
Contributors: Meng, W., Jiang, L., Wang, Y., Li, J., Zhang, J., Xiang, Y.
Number of pages: 13
Pages: 252-264
Publication date: 2018
Peer-reviewed: Yes
Web of Science (2011): Impact factor 0.868
ISI indexed (2011): ISI indexed yes
BFI (2010): BFI-level 1
Scopus rating (2010): SJR 0.464 SNIP 1.425
Web of Science (2010): Impact factor 0.889
BFI (2009): BFI-level 1
Scopus rating (2009): SJR 0.514 SNIP 1.772
Web of Science (2009): Indexed yes
BFI (2008): BFI-level 1
Scopus rating (2008): SJR 0.536 SNIP 1.263
Scopus rating (2007): SJR 0.795 SNIP 1.62
Scopus rating (2006): SJR 0.584 SNIP 1.644
Scopus rating (2005): SJR 0.518 SNIP 2.075
Scopus rating (2004): SJR 0.33 SNIP 1.453
Scopus rating (2003): SJR 0.279 SNIP 1.885
Scopus rating (2002): SJR 0.163 SNIP 0.689
Scopus rating (2001): SJR 0.158 SNIP 0.281
Scopus rating (2000): SJR 0.218 SNIP 0.849
Scopus rating (1999): SJR 0.219 SNIP 0.784

Original language: English
Keywords: Charging threat, Mobile security, Smartphone privacy, Android and iOS device, Juice filming charging attack, Detection mechanism

DOIs:
10.1016/j.cose.2017.11.012
Source: FindIt
Source-ID: 2393672678
Research output: Research - peer-review › Journal article – Annual report year: 2018

**TMGMap: Designing Touch Movement-Based Geographical Password Authentication on Smartphones**

Although textual passwords are the most widely adopted authentication method, they are vulnerable to many known limitations. Graphical password is considered as one alternative to complement the existing authentication systems, based on the observation that humans can remember images better than textual information. In order to obtain a large password space, geographical passwords have received much attention, which enable users to select one or more places on a map for authentication. For example, PassMap requires users to choose two places on a world map as their credentials, and GeoPass enables users to click only one place for authentication. However, we identify that users are able to perform more particular gestures like touch movement on mobile devices as compared to a common computer. Motivated by the observation, in this work, we develop TMGMap, a touch movement-based geographical password scheme on smartphones, which allows users to draw their secrets on a world map via touch movement events. We conducted a user study with a total of 60 participants, and found that users could achieve better results with our scheme in the aspects of both security and usability, as compared to similar schemes.

**General information**
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Nanjing University of Aeronautics and Astronautics
Contributors: Meng, W., Liu, Z.
Pages: 373-390
Publication date: 2018

**Host publication information**
Title of host publication: Information Security Practice and Experience
Publisher: Springer
ISBN (Print): 9783319998060
(Lecture Notes in Computer Science, Vol. 11125).
Keywords: Computer Science, Systems and Data Security, Graphical password, Smartphone security, User authentication, Touch dynamics, Biometric authentication
DOIs:
10.1007/978-3-319-99807-7_23
Source: FindIt
Source-ID: 2439314673
TouchWB: Touch behavioral user authentication based on web browsing on smartphones

Modern mobile devices especially smartphones have rapidly evolved and are widely adopted by people of different ages. Smartphones can assist users in a variety of activities, i.e., from social networking to online shopping, but also have become an attractive target for cyber-criminals due to the stored personal data and sensitive information. The traditional authentication mechanisms like PIN suffer from well-known limitations and drawbacks in the security community; thus, touch behavioral authentication has recently received much attention. Intuitively, authentication based on free touches would be hard to build a stand-alone system. In this work, we advocate that such authentication can consider users' actions under certain phone applications like web browser, and then propose a touch gesture-based authentication scheme, called TouchWB, with 21 features that can be extracted from web browsing gestures. For evaluation, we implemented the scheme on Android phones and conducted a user study involving 48 participants. Experimental results demonstrated that our approach could reduce the touch behavioral deviation by nearly half and achieve an average error rate of about 2.4% by using a combined classifier of PSO-RBFN.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Guangzhou University, Hong Kong Applied Science and Technology Research Institute, Swinburne University of Technology
Contributors: Meng, W., Wang, Y., Wong, D. S., Wen, S., Xiang, Y.
Number of pages: 9
Pages: 1-9
Publication date: 2018
Peer-reviewed: Yes

Publication information
Journal: Journal of Network and Computer Applications
Volume: 117
ISSN (Print): 1084-8045
Ratings:
BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 1
Scopus rating (2017): CiteScore 5.13 SJR 0.784 SNIP 2.401
Web of Science (2017): Impact factor 3.991
Web of Science (2017): Indexed yes
BFI (2016): BFI-level 1
Scopus rating (2016): CiteScore 4.42 SJR 0.728 SNIP 2.486
Web of Science (2016): Impact factor 3.5
BFI (2015): BFI-level 1
Scopus rating (2015): CiteScore 3.98 SJR 0.775 SNIP 2.665
Web of Science (2015): Impact factor 2.331
BFI (2014): BFI-level 1
Scopus rating (2014): CiteScore 3.82 SJR 0.878 SNIP 2.943
Web of Science (2014): Impact factor 2.229
BFI (2013): BFI-level 1
Scopus rating (2013): CiteScore 3.21 SJR 0.69 SNIP 2.741
Web of Science (2013): Impact factor 1.772
BFI (2012): BFI-level 1
Scopus rating (2012): CiteScore 2.48 SJR 0.537 SNIP 2.028
Web of Science (2012): Impact factor 1.467
BFI (2011): BFI-level 1
Scopus rating (2011): CiteScore 1.97 SJR 0.438 SNIP 1.896
Web of Science (2011): Impact factor 1.065
BFI (2010): BFI-level 1
Scopus rating (2010): SJR 0.388 SNIP 1.022
Web of Science (2010): Impact factor 0.66
BFI (2009): BFI-level 1
Towards Bayesian-based Trust Management for Insider Attacks in Healthcare Software-Defined Networks

The medical industry is increasingly digitalized and Internet-connected (e.g., Internet of Medical Things), and when deployed in an Internet of Medical Things environment, software-defined networks (SDN) allow the decoupling of network control from the data plane. There is no debate among security experts that the security of Internet-enabled medical devices is crucial, and an ongoing threat vector is insider attacks. In this paper, we focus on the identification of insider attacks in healthcare SDNs. Specifically, we survey stakeholders from 12 healthcare organizations (i.e., two hospitals and two clinics in Hong Kong, two hospitals and two clinics in Singapore, and two hospitals and two clinics in China). Based on the survey findings, we develop a trust-based approach based on Bayesian inference to figure out malicious devices in a healthcare environment. Experimental results in either a simulated and a real-world network environment demonstrate the feasibility and effectiveness of our proposed approach regarding the detection of malicious healthcare devices, i.e., our approach could decrease the trust values of malicious devices faster than similar approaches.

General information

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, University of Texas, University of Plymouth, Luleå University of Technology
Contributors: Meng, W., Choo, K. R., Furnell, S., Vasilakos, A. V., Probst, C. W.
Number of pages: 13
Pages: 761-773
Publication date: 2018
Peer-reviewed: Yes

Publication information
Journal: IEEE Transactions on Network and Service Management
Volume: 15
Issue number: 2
ISSN (Print): 1932-4537
Ratings:
BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 1
Scopus rating (2017): CiteScore 4.38 SJR 0.63 SNIP 2.056
Web of Science (2017): Impact factor 3.286
Web of Science (2017): Indexed yes
BFI (2016): BFI-level 1
Scopus rating (2016): CiteScore 4.02 SJR 0.663 SNIP 2.251
Web of Science (2016): Impact factor 3.134
BFI (2015): BFI-level 1
Towards False Alarm Reduction using Fuzzy If-Then Rules for Medical Cyber Physical Systems

Cyber-Physical Systems (CPS) are integrations of computation, networking and physical processes. Its process control is often referred to as embedded systems. Generally, CPS and Internet of Things (IoT) have the same basic architecture, whereas the former shows a higher combination and coordination between physical and computational elements, i.e., wireless sensor networks (WSNs) can be a vital part of CPS applications. With the rapid development, CPS has been applied to healthcare industry, where a wide range of medical sensors are used within a healthcare organization. However, these sensors may generate a large number of false alarms in practice, which could significantly reduce the system effectiveness. Targeting on this issue, in this work, we attempt to design a Medical Fuzzy Alarm Filter (named MFAFilter) for healthcare environments by means of fuzzy logic, especially fuzzy if-then rules, which could handle the vague and imprecise among data. In the evaluation, we conducted two major experiments to explore the performance of our approach in a simulated and a real network environment, respectively. Experimental results demonstrate that the use of fuzzy if-then rules could achieve a better accuracy as compared to the traditional supervised algorithms, and that our designed filter is effective in the practical environment.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, University of Hong Kong, University of Aizu
Contributors: Li, W., Meng, W., Su, C., Kwok, L. F.
Pages: 6530-6539
Publication date: 2018
Peer-reviewed: Yes

Publication information
Journal: IEEE Access
Volume: 6
ISSN (Print): 2169-3536
Ratings:
Web of Science (2018): Indexed yes
Scopus rating (2017): CiteScore 4.49
Web of Science (2017): Impact factor 3.557
Towards Securing Challenge-Based Collaborative Intrusion Detection Networks via Message Verification

With the increasing number of Internet-of-Things (IoT) devices, intrusion detection systems (IDSs) have been widely deployed in a distributed or collaborative setting, in which a collaborative intrusion detection network (CIDN) improves the detection accuracy of a single IDS by enabling IDS nodes to exchange useful information with each other. To protect CIDNs against insider attacks, challenge-based trust mechanisms are one promising solution to detect malicious nodes through sending challenges. However, several studies have revealed that this kind of mechanism is still vulnerable to some advanced insider attacks like passive message fingerprint attack (PMFA). Motivated by this observation, in this work, we focus on enhancing the security of challenge-based CIDNs and propose a compact but efficient message verification approach to defeat such insider attack by inserting a verifying alarm into each normal request. In the evaluation, we investigate the attack performance under both simulated and real network environments. Experimental results demonstrate that our approach can identify malicious nodes under PMFA and decrease their trust values in a quick manner.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, City University of Hong Kong, University of Surrey, Guangzhou University
Contributors: Li, W., Meng, W., Wang, Y., Han, J., Li, J.
Pages: 313-328
Publication date: 2018

Host publication information
Title of host publication: Information Security Practice and Experience
ISSN (Print): 9783319998060
(Lecture Notes in Computer Science, Vol. 11125).
Keywords: Computer Science, Systems and Data Security, Intrusion detection, Collaborative network, Insider attack, Passive message fingerprint attack, Challenge-based trust mechanism
DOIs:
10.1007/978-3-319-99807-7_19
Source: FindIt
Source-ID: 2439314705
Research output: Research - peer-review › Article in proceedings – Annual report year: 2018

When Intrusion Detection Meets Blockchain Technology: A Review

With the purpose of identifying cyber threats and possible incidents, intrusion detection systems (IDSs) are widely deployed in various computer networks. In order to enhance the detection capability of a single IDS, collaborative intrusion detection networks (or collaborative IDSs) have been developed, which allow IDS nodes to exchange data with each other. However, data and trust management still remain two challenges for current detection architectures, which may degrade the effectiveness of such detection systems. In recent years, blockchain technology has shown its adaptability in many fields such as supply chain management, international payment, interbanking and so on. As blockchain can protect the integrity of data storage and ensure process transparency, it has a potential to be applied to intrusion detection domain. Motivated by this, this work provides a review regarding the intersection of IDSs and blockchains. In particular, we introduce the background of intrusion detection and blockchain, discuss the applicability of blockchain to intrusion detection, and identify open challenges in this direction.
A bayesian inference-based detection mechanism to defend medical smartphone networks against insider attacks

With the increasing digitization of the healthcare industry, a wide range of devices (including traditionally non-networked medical devices) are Internet- and inter-connected. Mobile devices (e.g. smartphones) are one common device used in the healthcare industry to improve the quality of service and experience for both patients and healthcare workers, and the underlying network architecture to support such devices is also referred to as medical smartphone networks (MSNs). MSNs, similar to other networks, are subject to a wide range of attacks (e.g. leakage of sensitive patient information by a malicious insider). In this work, we focus on MSNs and present a compact but efficient trust-based approach using Bayesian inference to identify malicious nodes in such an environment. We then demonstrate the effectiveness of our approach in detecting malicious nodes by evaluating the deployment of our proposed approach in a real-world environment with two healthcare organizations.
Today’s computer users have to remember several passwords for each of their accounts. It is easily noticed that people may have difficulty in remembering multiple passwords, which result in a weak password selection. Previous studies have shown that recall success rates are not statistically dissimilar between textual passwords and graphical passwords. With the advent of map-based graphical passwords, this paper focuses on multiple password interference and presents a pilot study consisting of 60 participants to study the recall of multiple passwords between text passwords and map-based passwords under various account scenarios. Each participant has to create six distinct passwords for different account scenarios. It is found that participants in the map-based graphical password scheme could perform better than the textual password scheme in both short-term (one-hour session) and long term (after two weeks) password memorability tests.
(i.e., they made higher success rates). Our effort attempts to complement existing studies and stimulate more research on this issue.

**General information**
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Singapore University of Technology and Design, City University of Hong Kong, Institute for Infocomm Research
Contributors: Meng, W., Li, W., Lee, W., Jiang, L., Zhou, J.
Pages: 145-162
Publication date: 2017

**Host publication information**
Title of host publication: Applied Cryptography and Network Security
Volume: 10355
Publisher: Springer
ISBN (Print): 9783319612034
(Lecture Notes in Computer Science, Vol. 10355).
Keywords: Computer Science, Systems and Data Security, Data Encryption, Security, Computer Communication Networks, Software Engineering, Information Systems Applications (incl. Internet), User authentication, Graphical passwords, Usable security, Multiple password interference, HCI
DOIs: 10.1007/978-3-319-61204-1_8
Source: FindIt
Source-ID: 2372498502
Research output: Research - peer-review › Article in proceedings – Annual report year: 2017

**A Privacy-Preserving Framework for Collaborative Intrusion Detection Networks Through Fog Computing**
Nowadays, cyber threats (e.g., intrusions) are distributed across various networks with the dispersed networking resources. Intrusion detection systems (IDSs) have already become an essential solution to defend against a large amount of attacks. With the development of cloud computing, a modern IDS is able to implement more complicated detection algorithms by offloading the expensive operations such as the process of signature matching to the cloud (i.e., utilizing computing resources from the cloud). However, during the detection process, no party wants to disclose their own data especially sensitive information to others for privacy concerns, even to the cloud side. For this sake, privacy-preserving technology has been applied to IDSs, while it still lacks of proper solutions for a collaborative intrusion detection network (CIDN) due to geographical distribution. A CIDN enables a set of dispersed IDS nodes to exchange required information. With the advent of fog computing, in this paper, we propose a privacy-preserving framework for collaborative networks based on fog devices. Our study shows that the proposed framework can help reduce the workload on cloud’s side.

**General information**
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Guangzhou University, City University of Hong Kong, Technical University of Denmark
Contributors: Wang, Y., Xie, L., Li, W., Meng, W., Li, J.
Pages: 267-279
Publication date: 2017

**Host publication information**
Title of host publication: Cyberspace Safety and Security: 9th International Symposium, CSS 2017, Xi’an China, October 23–25, 2017, Proceedings
Volume: 10581
Publisher: Springer
Edition: 1
ISBN (Print): 978-3-319-69470-2
ISBN (Electronic): 978-3-319-69471-9
(Lecture Notes in Computer Science).
Keywords: Collaborate network, Privacy preserving, Intrusion detection, Cloud environment, Fog computing
DOIs: 10.1007/978-3-319-69471-9_20
Source: FindIt
Source-ID: 2392385676
Research output: Research - peer-review › Article in proceedings – Annual report year: 2017
Detecting Malicious Nodes in Medical Smartphone Networks Through Euclidean Distance-Based Behavioral Profiling

With the increasing digitization of the healthcare industry, a wide range of medical devices are Internet- and interconnected. Mobile devices (e.g., smartphones) are one common facility used in the healthcare industry to improve the quality of service and experience for both patients and healthcare personnel. The underlying network architecture to support such devices is also referred to as medical smartphone networks (MSNs). Similar to other networks, MSNs also suffer from various attacks like insider attacks (e.g., leakage of sensitive patient information by a malicious insider). In this work, we focus on MSNs and design a trust-based intrusion detection approach through Euclidean distance-based behavioral profiling to detect malicious devices (or called nodes). In the evaluation, we collaborate with healthcare organizations and implement our approach in a real simulated MSN environment. Experimental results demonstrate that our approach is promising in effectively identifying malicious MSN nodes.

Developing advanced fingerprint attacks on challenge-based collaborative intrusion detection networks

Traditionally, an isolated intrusion detection system (IDS) is vulnerable to various types of attacks. In order to enhance IDS performance, collaborative intrusion detection networks (CIDNs) are developed through enabling a set of IDS nodes to communicate with each other. Due to the distributed network architecture, insider attacks are one of the major threats. In the literature, challenge-based trust mechanisms have been built to identify malicious nodes by evaluating the satisfaction levels between challenges and responses. However, such mechanisms rely on two major assumptions, which may result in a weak threat model. In this case, CIDNs may be still vulnerable to advanced insider attacks in real-world deployment. In this paper, we propose a novel collusion attack, called passive message fingerprint attack (PMFA), which can collect messages and identify normal requests in a passive way. In the evaluation, we explore the attack performance under both simulated and real network environments. Experimental results demonstrate that our attack can help malicious nodes send malicious responses to normal requests, while maintaining their trust values.
Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management model

To defend against complex attacks, collaborative intrusion detection networks (CIDNs) have been developed to enhance the detection accuracy, which enable an IDS to collect information and learn experience from others. However, this kind of networks is vulnerable to malicious nodes which are utilized by insider attacks (e.g., betrayal attacks). In our previous research, we developed a notion of intrusion sensitivity and identified that it can help improve the detection of insider attacks, whereas it is still a challenge for these nodes to automatically assign the values. In this article, we therefore aim to design an intrusion sensitivity-based trust management model that allows each IDS to evaluate the trustworthiness of others by considering their detection sensitivities, and further develop a supervised approach, which employs machine learning techniques to automatically assign the values of intrusion sensitivity based on expert knowledge. In the evaluation, we compare the performance of three different supervised classifiers in assigning sensitivity values and investigate our trust model under different attack scenarios and in a real wireless sensor network. Experimental results indicate that our trust model can enhance the detection accuracy of malicious nodes and achieve better performance as compared with similar models.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, City University of Hong Kong
Contributors: Li, W., Meng, W., Kwok, L., IP, H. H.
Number of pages: 11
Pages: 135-145
Publication date: 2017
Enhancing Trust Management for Wireless Intrusion Detection via Traffic Sampling in the Era of Big Data

Internet of Things (IoT) has been widely used in our daily life, which enables various objects to be interconnected for data exchange, including physical devices, vehicles, and other items embedded with network connectivity. Wireless sensor network (WSN) is a vital application of IoT, providing many kinds of information among sensors, whereas such network is vulnerable to a wide range of attacks, especially insider attacks, due to its natural environment and inherent unreliable transmission. To safeguard its security, intrusion detection systems (IDSs) are widely adopted in a WSN to defend against insider attacks through implementing proper trust-based mechanisms. However, in the era of big data, sensors may generate excessive information and data, which could degrade the effectiveness of trust computation. In this paper, we focus on this challenge and propose a way of combining Bayesian-based trust management with traffic sampling for wireless intrusion detection under a hierarchical structure. In the evaluation, we investigate the performance of our approach in both a simulated and a real network environment. Experimental results demonstrate that packet-based trust management would become ineffective in a heavy traffic environment, and that our approach can help lighten the burden of IDSs in handling traffic while maintaining the detection of insider attacks.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Technical University of Denmark, University of Aizu, Singapore University of Technology and Design, University of New Brunswick
Contributors: Meng, W., Li, W., Su, C., Zhou, J., Lu, R.
Pages: 7234 - 7243
Publication date: 2017
Peer-reviewed: Yes

Publication information
Journal: IEEE Access
Volume: 6
ISSN (Print): 2169-3536
Ratings:
BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 1
Scopus rating (2017): CiteScore 4.49
Web of Science (2017): Impact factor 3.557
Web of Science (2017): Indexed yes
BFI (2016): BFI-level 1
Scopus rating (2016): CiteScore 5.13
Web of Science (2016): Impact factor 3.244
BFI (2015): BFI-level 1
Scopus rating (2015): CiteScore 4.32
Web of Science (2015): Impact factor 1.27
BFI (2014): BFI-level 1
Scopus rating (2014): CiteScore 3.16
BFI (2013): BFI-level 1
Original language: English
Keywords: Bayesian Model, Big Data, Intrusion Detection, Traffic Sampling, Trust Computation, Wireless Sensor Network
Electronic versions:
08105800.pdf
DOIs:
10.1109/ACCESS.2017.2772294
Source: FindIt
Source-ID: 2394676400
Research output: Research - peer-review ; Journal article – Annual report year: 2018

Evaluating challenge-based trust mechanism in medical smartphone networks: an empirical study

Intrusion detection systems (IDSs) are one of the widely adopted security tools in protecting computer networks, whereas it is still a big challenge for a single IDS to identify various threats in practice. Collaborative intrusion detection networks (CIDNs) are then developed in order to enhance the detection capability of a single IDS. However, CIDNs are known to suffer from insider attacks, in which malicious nodes can perform adversary actions. To mitigate this issue, challenge-based trust mechanisms are one of the promising solutions in literature, which are robust against various common insider threats. With the popularity of mobile devices, medical smartphone networks (MSNs) have become an emerging network architecture for healthcare organizations to improve the quality of medical services. Due to the sensitivity, there is a great
need to defend MSNs against insider attacks. In this work, we conduct an empirical study to investigate and evaluate the implementation of challenge-based mechanism in MSNs. Our work aims to complement current literature, through providing insights and learned lessons (i.e., whether it is suitable to deploy such a mechanism in MSNs).

Exploring Effect of Location Number on Map-Based Graphical Password Authentication
Graphical passwords (GPs) that authenticate users using images are considered as one potential alternative to overcome the issues of traditional textual passwords. Based on the idea of utilizing an extremely large image, map-based GPs like PassMap and GeoPass have been developed, where users can select their secrets (geographical points) on a world map. In particular, PassMap allows users to select two locations on a map, while GeoPass reduces the number of locations to only one. At first glance, selecting one location is more vulnerable to attacks, while increasing the location number may add burden on users. In the literature, there is no research exploring this issue. Motivated by this, our purpose in this work is to explore the effect of location number (the number of geographical points) and compare two schemes of PassMap and GeoPass in terms of users’ performance and feedback. In this work, we develop a generic and open platform for realizing map-based schemes, and conduct a user study with 60 participants. The study reveals that selecting two locations would not degrade the scheme performance. Our effort aims to complement exiting research studies in this area.

Exploring Energy Consumption of Juice Filming Charging Attack on Smartphones: A Pilot Study
With the increasing demand of smartphone charging, more and more public charging stations are under construction (e.g., airports, subways, shops). This scenario may expose a good chance for cybercriminals to launch charging attacks and steal user’s private information. Juice filming charging (JFC) attack is one example, which can steal users’ sensitive information from both Android OS and iOS devices, through automatically recording phone-screen information and the
user inputs during the charging process. The rationale is that users' information can be leaked through a standard micro USB connector that employs the Mobile High-Definition Link (MHL) standard. Motivated by the potential damage of charging attack, we focus on JFC attack in this paper, and investigate for the first time the energy consumption, especially CPU usage caused by JFC attack. In particular, we conduct a user study with over 500 participants and identify that JFC attack may increase CPU usage when connecting the phone to the malicious charger, but this anomaly is hard for raising the attention from a common user. Our work aims to complement existing state-of-the-art results, raise more attention and stimulate more research on charging attacks.

**General information**
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Guangzhou University, University of Aizu
Contributors: Jiang, L., Meng, W., Wang, M. Y., Su, C., Li, J.
Pages: 199-213
Publication date: 2017

**Host publication information**
Title of host publication: Network and System Security 2017
Volume: 10394
Publisher: Springer
ISBN (Print): 9783319647005
(Lecture Notes in Computer Science, Vol. 10394).
Keywords: Computer Science, Systems and Data Security, Computer Communication Networks, Data Encryption, Management of Computing and Information Systems, Software Engineering, Information Systems Applications (incl. Internet), Emerging threats, Mobile privacy and security, User study, Android and iOS, Juice filming charging attack, USB cable
DOIs:
10.1007/978-3-319-64701-2_15
Source: FindIt
Source-ID: 2372953630
Research output: Research - peer-review › Article in proceedings – Annual report year: 2017

Harvesting Smartphone Privacy Through Enhanced Juice Filming Charging Attacks
The increasingly high demand for smartphone charging in people’s daily lives has apparently encouraged much more public charging stations to be deployed in various places (e.g., shopping malls, airports). However, these public charging facilities may open a hole for cyber-criminals to infer private information and data from smartphone users. Juice filming charging (JFC) attack is a particular type of charging attacks, which is capable of stealing users' sensitive information from both Android OS and iOS devices, through automatically monitoring and recording phone screen during the whole charging period. The rationale is that phone screen can be leaked through a standard micro USB connector, which adopts the Mobile High-Definition Link (MHL) standard. In practice, we identify that how to efficiently extract information from the captured videos remains a challenge for current JFC attack. To further investigate its practical influence, in this work, we focus on enhancing its performance in the aspects of extracting texts from images and correlating information, and then conducting a user study in a practical scenario. The obtained results demonstrate that our enhanced JFC attack can outperform the original one in collecting users' information at large and extracting sensitive data with a higher accuracy. Our work aims to complement existing results and stimulate more efforts in defending smartphones against charging threats.

**General information**
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Technical University of Denmark, City University of Hong Kong, Hong Kong Polytechnic University
Contributors: Meng, W., Fei, F., Li, W., Au, M. H.
Number of pages: 18
Pages: 291-308
Publication date: 2017

**Host publication information**
Title of host publication: Information Security
Volume: 10599
Publisher: Springer
ISBN (Print): 978-3-319-69658-4
ISBN (Electronic): 978-3-319-69659-1
(Lecture Notes in Computer Science, Vol. 10599).
Keywords: Mobile privacy and security, Android and iOS, Charging threat, OCR technology, Juice filming charging attack
DOIs:
SOOA: Exploring Special On-Off Attacks on Challenge-Based Collaborative Intrusion Detection Networks
The development of collaborative intrusion detection networks (CIDNs) aims to enhance the performance of a single intrusion detection system (IDS), through communicating and collecting information from other IDS nodes. To defend CIDNs against insider attacks, trust-based mechanisms are crucial for evaluating the trustworthiness of a node. In the literature, challenge-based trust mechanisms are well established to identify malicious nodes by identifying the deviation between challenges and responses. However, such mechanisms rely on two major assumptions, which may result in a weak threat model and render CIDNs still vulnerable to advanced insider attacks in a practical deployment. In this paper, our motivation is to investigate the effect of On-Off attacks on challenge-based CIDNs. In particular, as a study, we explore a special On-Off attack (called SOOA), which can keep responding normally to one node while acting abnormally to another node. In the evaluation, we explore the attack performance under simulated CIDN environments. Experimental results indicate that our attack can interfere the effectiveness of trust computation for CIDN nodes.

General Information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, City University of Hong Kong
Contributors: Li, W., Meng, W., Kwok, L.
Pages: 402-415
Publication date: 2017

Host publication information
Title of host publication: Green, Pervasive, and Cloud Computing
Volume: 10232
Publisher: Springer
ISBN (Print): 9783319571850
(Lecture Notes in Computer Science, Vol. 10232).
Keywords: Computer Science, Computer Communication Networks, Information Systems Applications (incl. Internet), Software Engineering, Information Storage and Retrieval, Algorithm Analysis and Problem Complexity, Artificial Intelligence (incl. Robotics), Intrusion Detection System, Collaborative network, On-off attacks, Challenge-based CIDN, Trust management
DOIs:
10.1007/978-3-319-57186-7_30
Source: FindIt
Source-ID: 2372482464
Research output: Research - peer-review › Article in proceedings – Annual report year: 2017

Towards effective and robust list-based packet filter for signature-based network intrusion detection: an engineering approach
Network intrusion detection systems (NIDSs) which aim to identify various attacks, have become an essential part of current security infrastructure. In particular, signature-based NIDSs are being widely implemented in industry due to their low rate of false alarms. However, the signature matching process is a big challenge for these systems, in which the cost is at least linear to the size of an input string. As a result, overhead packets will be a major issue for practical usage, where the incoming packets exceed the maximum capability of an intrusion detection system (IDS). To mitigate this problem, packet filtration is a promising solution to reduce unwanted traffic. Motivated by this, in this work, a list-based packet filter was designed and an engineering method of combining both blacklist and whitelist techniques was introduced. To further secure such filters against IP spoofing attacks, a lightweight but efficient IP verification mechanism was developed. In the evaluation, a list-based packet filter was deployed in both simulated and real network environments under honest and dishonest scenarios. Experimental results demonstrate that the developed list-based packet filter is effective in traffic filtration as well as workload reduction, and is robust against IP spoofing attacks.

General Information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, University of Hong Kong
Contributors: Meng, W., Li, W., Kwok, L. F.
Number of pages: 12
Pages: 204-215
Publication date: 2017
Peer-reviewed: Yes
Towards Effective Trust-Based Packet Filtering in Collaborative Network Environments

Overhead network packets are a big challenge for intrusion detection systems (IDSs), which may increase system burden, degrade system performance, and even cause the whole system collapse, when the number of incoming packets exceeds the maximum handling capability. To address this issue, packet filtration is considered as a promising solution, and our previous research efforts have proven that designing a trust-based packet filter was able to refine unwanted network packets and reduce the workload of a local IDS. With the development of Internet cooperation, collaborative intrusion detection environments (e.g., CIDNs) have been developed, which allow IDS nodes to collect information and learn experience from others. However, it would not be effective for the previously built trust-based packet filter to work in such a collaborative environment, since the process of trust computation can be easily compromised by insider attacks. In this paper, we adopt the existing CIDN framework and aim to apply a collaborative trust-based approach to reduce unwanted packets. More specifically, we develop a collaborative trust-based packet filter, which can be deployed in collaborative networks and be robust against typical insider attacks (e.g., betrayal attacks). Experimental results in various simulated and practical environments demonstrate that our filter can perform effectively in reducing unwanted traffic and can defend against insider attacks through identifying malicious nodes in a quick manner, as compared to similar approaches.
Towards enhancing click-draw based graphical passwords using multi-touch behaviours on smartphones

Graphical passwords (GPs) are recognised as one of the potential alternatives in addressing the limitations in conventional text-based password authentication. With the rapid development of mobile devices (i.e., the increase of computing power), GP-based systems have already been implemented not only on PCs, but also on smartphones to authenticate legitimate users and detect impostors. However, as compared to common computers, we identify that users are able to perform some distinct actions like multi-touch on smartphones. The multi-touch is a distinguished feature on current smartphones and its impact on graphical password creation is an important topic in the literature. In this paper, our interest is to investigate the influence of multi-touch behaviours on users’ habit in creating graphical passwords, especially on click-draw based GPs (shortly CD-GPS) on mobile devices. In the evaluation, we develop a multi-touch enabled CD-GPS on smartphones and conduct two major experiments with a total of 90 participants. The study results indicate that participants are more likely to use multi-touch features to create their secrets, and multi-touch can make a positive impact on creating graphical passwords (i.e., offering higher success rates and less time consumption).

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, City University of Hong Kong, University of Texas at San Antonio
Contributors: Meng, W., Li, W., Kwok, L. F., Choo, K. K. R.
Pages: 213-229
Publication information
Journal: Computers & Security
Volume: 65
ISSN (Print): 0167-4048
Ratings:
BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 1
Scopus rating (2017): CiteScore 3.86 SJR 0.684 SNIP 2.158
Web of Science (2017): Impact factor 2.65
Web of Science (2017): Indexed yes
BFI (2016): BFI-level 1
Scopus rating (2016): CiteScore 3.59 SJR 0.815 SNIP 2.158
Web of Science (2016): Impact factor 2.849
BFI (2015): BFI-level 1
Scopus rating (2015): CiteScore 3.03 SJR 0.819 SNIP 2.346
Web of Science (2015): Impact factor 1.64
BFI (2014): BFI-level 1
Scopus rating (2014): CiteScore 2.39 SJR 0.641 SNIP 2.133
Web of Science (2014): Impact factor 1.031
BFI (2013): BFI-level 1
Scopus rating (2013): CiteScore 2.48 SJR 0.697 SNIP 2.601
Web of Science (2013): Impact factor 1.172
ISI indexed (2013): ISI indexed yes
BFI (2012): BFI-level 1
Scopus rating (2012): CiteScore 2.56 SJR 0.68 SNIP 2.475
Web of Science (2012): Impact factor 1.158
ISI indexed (2012): ISI indexed yes
BFI (2011): BFI-level 1
Scopus rating (2011): CiteScore 2.44 SJR 0.518 SNIP 2.146
Web of Science (2011): Impact factor 0.868
ISI indexed (2011): ISI indexed yes
BFI (2010): BFI-level 1
Scopus rating (2010): SJR 0.464 SNIP 1.425
Web of Science (2010): Impact factor 0.889
BFI (2009): BFI-level 1
Scopus rating (2009): SJR 0.514 SNIP 1.772
Web of Science (2009): Indexed yes
BFI (2008): BFI-level 1
Scopus rating (2008): SJR 0.536 SNIP 1.263
Scopus rating (2007): SJR 0.795 SNIP 1.62
Scopus rating (2006): SJR 0.584 SNIP 1.644
Scopus rating (2005): SJR 0.518 SNIP 2.075
Scopus rating (2004): SJR 0.33 SNIP 1.453
Scopus rating (2003): SJR 0.279 SNIP 1.885
Scopus rating (2002): SJR 0.163 SNIP 0.689
Scopus rating (2001): SJR 0.158 SNIP 0.281
Scopus rating (2000): SJR 0.218 SNIP 0.849
Scopus rating (1999): SJR 0.219 SNIP 0.784
Original language: English
Keywords: Graphical passwords, User authentication on, Smartphones, Multi-touch, Human factors, Mobile security
DOIs:
Towards Statistical Trust Computation for Medical Smartphone Networks Based on Behavioral Profiling
Due to the popularity of mobile devices, medical smartphone networks (MSNs) have been evolved, which become an emerging network architecture in healthcare domain to improve the quality of service. There is no debate among security experts that the security of Internet-enabled medical devices is woefully inadequate. Although MSNs are mostly internally used, they still can leak sensitive information under insider attacks. In this case, there is a need to evaluate a node’s trustworthiness in MSNs based on the network characteristics. In this paper, we focus on MSNs and propose a statistical trust-based intrusion detection mechanism to detect malicious nodes in terms of behavioral profiling (e.g., camera usage, visited websites, etc.). Experimental results indicate that our proposed mechanism is feasible and promising in detecting malicious nodes under medical environments.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Hong Kong Polytechnic University
Contributors: Meng, W., Au, M. H.
Pages: 152–159
Publication date: 2017

PMFA: Toward Passive Message Fingerprint Attacks on Challenge-Based Collaborative Intrusion Detection Networks
To enhance the performance of single intrusion detection systems (IDSs), collaborative intrusion detection networks (CIDNs) have been developed, which enable a set of IDS nodes to communicate with each other. In such a distributed network, insider attacks like collusion attacks are the main threat. In the literature, challenge-based trust mechanisms have been established to identify malicious nodes by evaluating the satisfaction between challenges and responses. However, we find that such mechanisms rely on two major assumptions, which may result in a weak threat model and make CIDNs still vulnerable to advanced insider attacks in practical deployment. In this paper, we design a novel type of collusion attack, called passive message fingerprint attack (PMFA), which can collect messages and identify normal requests in a passive way. In the evaluation, we explore the attack performance under both simulated and real network environments. Experimental results indicate that under our attack, malicious nodes can send malicious responses to normal requests while maintaining their trust values.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, City University of Hong Kong
Contributors: Li, W., Meng, W., Kwok, L., Ip, H. S.
Pages: 433–449
Publication date: 2016
Smartphone User Authentication Using Touch Dynamics in the Big Data Era: Challenges and Opportunities

With the wide adoption of smartphones, touchscreens have become the leading input method on the mobile platform, with more than 78% of all phones using a touchscreen. Thus, more research studies started focusing on touch dynamics and its applications on user authentication. Generally, touch dynamics can be described as the characteristics of the inputs received from a touchscreen when a user is interacting with a device (e.g., a touchscreen mobile phone). Intuitively, touch dynamics is different from keystroke dynamics in that touch dynamics has more input types such as multi-touch and touch movement. On the other hand, the inputs of press button up and press button down in keystroke dynamics are similar to the actions of touch press up and touch press down (e.g., single-touch) in touch dynamics. Due to its characteristics, touch dynamics received more attention from the literature. In this chapter, we aim to present a review, introducing recent advancement relating to touch dynamics in the literature, and providing insights about its future trends in the big data era.