At the Center of Innovation

CYBER at BGU

Spotlight on Excellence in Research

אוניברסיטת בן-גוריון בנגב
Ben-Gurion University of the Negev

CyberSpark members have the opportunity to partner with BGU's cyber laboratories with their proven track record of successful industry collaborations.

The Deutsche Telekom Innovation Labs at BGU have been at the forefront of mobile data protection for nearly a decade. Harnessing the innovative might of the telecommunications giant to the unconventional and inventive brainpower of BGU researchers has led to numerous breakthroughs and created an environment that fosters innovation in the field. BGU has demonstrated competencies in a wide range of fields including Mobile Network Security, Cross-Platform Malware Detection and Security Analytics and User Profiling for both private and public users. These are essential to ensure the protection of national infrastructures.

The INCB is working with BGU to establish a joint research enterprise that will focus on innovative cyber security applications.

Contact for more Information:
Zafrir Levy, Vice President
Business Development
Exact Sciences & Engineering
BGN Technologies
cyber@bgu.ac.il | Tel: +972-52-2565715

CYBER at **BGU**

Spotlight on Excellence in Research

Low Amplitude Anomaly Detection

Goals

Users in organizations regularly access various internal and external computational resources. Such user activity is logged as events by various devices (firewalls, DLP systems, IDSs, routers, antivirus, VPN, servers, etc.) These events are then collected by Security Information and Event Management (SIEM) systems for further processing and analysis in an attempt to detect cyber attacks. Specifically, users' behavioral profiles can be derived based on the collected events in order to detect anomalies or malicious activity.

Previous studies proposed and evaluated methods for intelligent data analysis, specifically profiling users' activity, in order to identify abnormal behavior. However, existing methods are incapable of dealing with advanced attacks that are able to "stay below the radar" and hide malicious activity within legitimate activity and thus evade such detection mechanisms.

Description

In this research we develop a method that is based on machine learning techniques combined with statistical analysis for deriving users' behavioral profiles based on the collected events in order to detect long term trends and anomalies (low amplitude anomalies).

While the collected events are always logged with the source IP address they are not always logged with the relevant username (used as the identifier) and therefore, many of the collected events are not directly linked with the appropriate user. In this research we also describe a method for associating an IP address with an actual username based on a set of logged events. This is a crucial precondition for generating an accurate user's profile. The proposed method was evaluated using real large datasets (logs) and showed 88% accuracy in the identification of usernames.

Researchers

Dr. Asaf Shabtai
shabtaia@bgu.ac.il

Prof. Lior Rokach
liorrk@bgu.ac.il

Prof. Yuval Elovici
elovici@bgu.ac.il

Publications

Shabtai, A., Morad, I., Kolman, E., Eran, E., Vaystikh, A., Gruss, E., Rokach, L., Elovici, Y. IP2User – Identifying the username of an IP Address in Network-Related Events", In Proc. of the 2nd IEEE BigData Congress, USA, 2013

Detecting Computers in Cyber Space Maliciously Exploited as SSH Proxies

Goals

SSH protocol may be maliciously exploited by hackers in order to hide the source, destination and nature of an attack. This can be done by enabling SSH tunneling to act as a proxy through which the malicious traffic is transmitted (e.g., leaking sensitive data, or command and control communications). As a case in point, the Flame virus detected in 2012 used SSL and SSH for stealing sensitive information and the Duqu virus detected in 2011 used SSH port forwarding to hide the command and control traffic and the IP of the control application.

Description

In this research we propose and evaluate a method, based on machine learning techniques, for detecting an SSH proxy server that is used to transmit malicious traffic.

Specifically, we aim to: identify tunneled SSH traffic, classify the application/protocol encrypted by the SSH tunnel and match (correlating) incoming/outgoing encrypted traffic.

Experiments conducted using servers deployed on Amazon Cloud proved able to detect tunneled traffic and to classify the tunneled protocol with sufficient accuracy.

For experimentation we used automatic tools for generating traffic of various protocols (HTTP, HTTPS, SMTP, POP3, IMAP, IRC, XMPP, SKYPE, TORRENT, plain SSH) and to extract network-based features.

Researchers

Dr. Asaf Shabtai
shabtaia@bgu.ac.il

Prof. Yuval Elovici
elovici@bgu.ac.il

Securing Android-Based Devices

Researchers

Dr. Asaf Shabtai
shabtaia@bgu.ac.il

Prof. Yuval Elovici
elovici@bgu.ac.il

Publications

Security evaluation
Asaf Shabtai, et al., "Google Android: A Comprehensive Security Assessment", *IEEE Security and Privacy*, Volume 8, Issue 2, Pages 35-44, March/April 2010

Intrusion detection
Asaf Shabtai, et al., "Andromaly: An Anomaly Detection Framework for Android Devices", *Journal of Intelligent Information Systems*, 38(1), 2012, 161-190

SELinux
Asaf Shabtai, Yuval Fledel, Yuval Elovici, "Securing Android-Powered Mobile Devices Using SELinux", *IEEE Security and Privacy*, Volume 8, Issue 3, Pages 36-44, May/June 2010

Goals

The "Securing Android-based Devices" research was conducted six months before the first Android-based mobile devices were distributed by T-Mobile USA. The main goal of the research was to gain essential knowledge regarding the security of the Android platform.

Description

In this research we acquired deep understanding of the Android framework and inherent security mechanisms and identified and evaluated a collection of applicable security solutions for Android.

During the research we carried out a methodological risk analysis process and identified high risk threats (vulnerability to SQL injection, Web attacks, partial code and configuration review, applicability of existing Java and Linux malware). We demonstrated attack scenarios including: developing malware (Denial of Service, PC malware injection), exploiting the Shared-User-ID feature and man-in-the-middle attack on the Android Market's (today, the Play store) protocol.

We demonstrated the applicability of various security solutions such as: SELinux, remotely configurable Firewall, activity-based verification, backup and recovery of applications, and static analysis of applications. In addition, we developed Andromaly, a powerful, modular and reusable intrusion detection framework for Android. We evaluated various Artificial Intelligence methods for detecting abnormal states (Machine Learning and Temporal Reasoning). The CPU consumption of the Andromaly application was in the interval 5.52%±2.11 and the battery measurements showed 10% degradation.

Customer Data Leakage Prevention

Goals

Protecting sensitive customer information from unauthorized disclosure is a major concern of every company. Since the company's employees need to access customer information, customer data leakage prevention is a very complex task.

Description

In this research we reviewed state-of-the-art commercial and academic data leakage prevention solutions. Then we developed and evaluated various data misuse detection methods which include:

Anomaly detection using a novel supervised and unsupervised context-based data linkage algorithm that is used to derive normal access patterns and detect abnormal access patterns that may indicate customer data leakage/misuse incidents.

M-Score – a Misuseability Weight measure that assigns a sensitivity rank to datasets accessed by employees which indicates the potential damage to the organization in the event that the data is misused.

Employ the concepts of **honeytokens** for detecting data misuse incidents, and answering questions such as how to use the honeytokens effectively, how to generate reliable honeytokens, and how many to create.

An improved **collaborative e-mail leakage prevention** method that analyzes the communication of groups of users.

In order to evaluate our proposed method we developed an evaluation environment and a detection system prototype.

Researchers

Dr. Asaf Shabtai
shabtaia@bgu.ac.il

Prof. Yuval Elovici
elovici@bgu.ac.il

Prof. Lior Rokach
liorrk@bgu.ac.il

Publications

Shabtai, A., Rokach, L., Elovici, Y., "A Survey of Data Leakage Detection and Prevention Solutions", SpringerBriefs in Computer Science, Springer.

Shabtai, A., et al. "Detecting Data Misuse by Monitoring Data Items", ACM *Transactions on Knowledge Discovery from Data (TKDD)*, 2014

Zilberman, et al., "Analyzing Group Emails Exchange for Detecting Data Leakage via Email", *Journal of the American Society for Information Science and Technology (JASIST)*, 64(9), 2013, 1780-1790

Gafny, M., et al., "OCCT: A One-Class Clustering Tree for One-to-Many Data Linkage", *IEEE Transactions on Knowledge and Data Engineering (TKDE)*, 2013(1)

Harel, A., et al., "M-score: A Misuseability Weight Measure", *IEEE Transactions on Dependable and Secure Computing*, 9(3), 2012, 414-428

Emerging Database Security Solutions

Goals

Emerging Database Security Solutions is a follow-up project to the "Next Generation Database Security" study, which was carried out in 2008. It aims at further research and development in three different areas and consequently inventing innovative database security solutions.

Description

Design secure database applications: System developers tend to neglect security requirements or to only deal with them at the end of the development process. There is no way to verify that security requirements are defined, validated and implemented. The project of developing Security Method and Tool within the scope of Emerging Database Security Solutions is intended to address these problems by developing a methodology and a supporting software tool that will force developers, in particular the database designers, to deal with database security requirements related to authorization in the early stages of development.

Anonymize exported data: Data holders have an obligation to protect a respondent's identity when releasing data about individuals. K-Anonymity is a model of protecting exported data in which each piece of disclosed data is equivalent to at least k-1 other pieces of disclosed data over a set of attributes that are deemed to be privacy sensitive. Existing K-Anonymity solutions either suffer from inefficiency, insufficient quality of preserved data, scarce data or the method requires prior domain knowledge to allow application to different databases. The new K-Anonymity algorithm shall correspond to designated requirements.

Smart database audit: Currently users usually receive a pooled connection to the database when accessing the database via a web server. It appears to the specific database that such a connection is always established by the same user (the web server itself). The Emerging Database Security Solutions project intends to develop a method called "Smart database audit" which enables the identification of the real user by the database. Identifying the real user by the database results in better logs, which entails better intrusion detection and prevention.

Researchers

Prof. Ehud Gudes
ehud@cs.bgu.ac.il

Dr. Erez Shmueli
shmueli@mit.edu

Context-Based Data Leakage Detection

Goals

In many cases, determining the overall subject of the text is not sufficient: a small section of confidential or sensitive text may be hidden in a larger, non-confidential one; understanding the context in which a term is used is sometimes as important as identifying this term. This problem is not fully addressed by existing algorithms.

Description

In this research we developed a novel graph based model that is capable of representing both the key terms in groups of document and the context in which they appear. This approach enables us to identify the meaning of specific terms, paragraphs and expressions instead of just analyzing the document as a whole.

As the research progressed, we refined the model. Today, instead of the fixed "rule based" approach that was employed in earlier versions we apply a machine-learning based approach, thus enabling the system itself to dynamically and independently define the detection rules and thresholds for each set of documents on which it is applied.

Researchers

Prof. Yuval Elovici
elovici@bgu.ac.il

Prof. Bracha Shapira
bshapira@bgu.ac.il

Gilad Katz
katzguka@bgu.ac.il

Publications

Katz, G., Elovici, Y. and Shapira B., "CoBAn: A Context Based Model for Data Leakage Prevention," accepted for publication in *Information Sciences, 2013*

Activity-based Verification Continuous User Verification after Successful Login

Researchers

Prof. Yuval Elovici
elovici@bgu.ac.il

Prof. Lior Rokach
liorrk@bgu.ac.il

Dr. Robert Moskovitch
robertmo@bgu.ac.il

Publications

Feher, C., Elovici, Y., Moskovitch, R., Rokach, L., & Schclar, A. (2012). "User identity verification via mouse dynamics." Information Sciences, 201, 19-36.

Shimshon, T., Moskovitch, R., Rokach, L., & Elovici, Y. (2010), Continuous verification using keystroke dynamics, IEEE International Conference on Computational Intelligence and Security (CIS), (pp. 411-415).

Schclar, A., Rokach, L., Abramson, A., & Elovici, Y. (2012). User Authentication Based on Representative Users. IEEE Transactions on SMC, 42(6), 1669-1678.

Description

Authentication vulnerability
The Internet and internal company applications currently require interacting with a multitude of identities and passwords since services such as email or eBanking use a mandatory login. Administering and maintaining this increasingly confusing multitude of access data, PINs, and TAN lists, however, is considered a bewildering and complex task, which leads users to often neglect security in favor of convenience.
Due to the misuse of user data, great financial damage is caused worldwide, both for the users and for the providers of products and services. Corresponding authorization credentials can get lost in any number of ways: through voluntary transmission, physical theft, or digital attacks such as phishing, sniffing, or Trojans. Another vulnerability of today's authentication mechanisms in Internet applications is the fact that users' identities are verified only at the start of every session.

Behavioral-based characteristics
Solutions that focus on behavioral-based characteristics for authentication are developed in the Activity-based Verification project. When interacting with the computer, every person generates individual activity patterns that can be saved as biometric signatures. Machine learning technologies can be used to recognize and analyze biometric characteristics. The underlying verification program must initially be trained for the respective user behavior. After logging in to a system, continuous verification will then be made on the basis of these specific biometric characteristics as to whether the logged in user remains the user of the system during the course of a session. For this, the system can use current typing behavior, mouse movements, or the operation of applications for comparison with the previously generated signatures. In the process, this ensures that authorized users are not disallowed and unauthorized users are not accepted.

Simpler and better security
Compared to physiological biometric characteristics (such as fingerprints, iris, etc.), behavioral-based biometric characteristics have the great advantage of being easily monitored without special hardware or modified user behavior. For example, password reset could be designed in a more user-friendly manner with activity-based verification. Instead of the current procedure, with which a temporary password is issued during registration with a service, the user would be prompted to transcribe a randomly selected word list. The biometric characteristics during the use of the keyboard would be evaluated and used for authentication.
Activity-based verification could also be used to replace transaction numbers (TANs) or hardware tokens that are currently required for online banking.

AccessDroid

Goals

The goal of the access-droid project was to develop an innovative push messaging service for developer-to-mobile communication.

The service focuses on Service-Level-Agreement (SLA), end-to-end security and developers' ease-of-use.

Description

Performance:

- Suitable for applications that heavily rely on push messaging.
- Operator friendly.
- Persistent communication channel over 3G, 4G and Wi-Fi optimized for energy efficiency and lowered modem signaling.

Security model:

- Message signing and encryption.
- Anti-pirating application authentication.
- Innovative obfuscation of private data onboard the device.

Reliability:

- Bounded maximum message delivery time.
- Assure message delivery.
- Prioritize messages.

Ease of use:

- Rich APIs for end-users (sender, receiver and admins) using cutting-edge technologies.
- Convenient default API implementations ready for organizational integration.

Researchers

Prof. Bracha Shapira
bshapira@bgu.ac.il

Prof. Shlomi Dolev
dolev@cs.bgu.ac.il

BizDroid

Researchers

Prof. Bracha Shapira
bshapira@bgu.ac.il

Prof. Yuval Elovici
elovici@bgu.ac.il

Publication

Bar, A., Mimran, D., Chekina, L., Elovici, Y., & Shapira, B. (2013, July). "Nesto-Network selection and traffic offloading system for android mobile devices". In Wireless Communications and Mobile Computing Conference (IWCMC), 2013 9th International (pp. 337-342). IEEE.

Messalem, G., Mimran, D., Dolev, S., Heimlich, I., Kopeetsky, M., Shapira, B., Elovici, Y., "Exploiting Simultaneous Usage of Different Wireless Interfaces for Security and Mobility," Proc. of the 2nd IEEE International Conference on Future Generation Communication Technologies, (FGCT), 2013.

Goals

Network selection and offloading system for Android-based mobile devices.

Providing a context aware "always best connected" (ABC) solution, selecting the best available network for each running application in different scenarios.

Description

Various supported policies: Energy Saving; Offloading; Browsing app; VOIP; Streaming; etc.

Dual Connection Mode – connecting to both 3G and WiFi networks simultaneously.

Multiple Attribute Decision Making models for selecting the best available networks according to the current state of the device.
Gradual Network Switching – shifting from one network to another seamlessly.

Results

Maximizing the relevant QoS features for each running application or scenario.

Dual Connection Mode improves the overall QoS measures compared to traditional network switching methods.

Flexibility to define effective hybrid policies, e.g.: maintaining good network delay values, while minimizing energy consumption.

Code Obfuscation

Goals

Research and develop generic dynamic obfuscation algorithms (transformations) for C/C++ programs. The obfuscation algorithms goal is to conceal the source programs` purpose and logic, and to protect them from being tampered or deter reverse engineered.

Description

We research two obfuscation algorithms. The first algorithm is responsible for bloating the programs` call-graph, whereas the second algorithm is responsible for diversifying the call-graph. The contribution of these two algorithms is two-fold. First, they augment the call-graph complexity by inserting large quantities of new vertices (functions). The second contribution is the ability to conceal most of the call-graph edges.

Consequently, these two obfuscation algorithms make the reverse-engineer task (done usually by an attacker) a much longer, tedious and difficult task.

Researchers

Prof. Yuval Elovici
elovici@bgu.ac.il

Prof. Lior Rokach
liorrk@bgu.ac.il

Prof. Bracha Shapira
bshapira@bgu.ac.il

Dr. Eitan Menahem
eitanme@bgu.ac.il

Automatic XML Context Learning

Goals

Currently, many information systems interact through XML files. These interactions may fall victim to one or more adversary attacks, including: information leakage, dictionary and buffer overflow attacks, cross-site scripting, SQL injection, parameter tampering and more.

The goal of this research is to study a new automated context learning method for producing a list of rules, which describes precisely the usable values ranges of the XML elements within the XML transactions. The studied algorithm allows to (1) decrease the XML attack-surface, and (2) classify XML transactions as abnormal or normal (i.e. attacked or not).

Description

The studied algorithm for automated context-learning XML can be used as an XML firewall to defend against most of the known XML attacks. The XML-firewall framework is divided into separate logical units: the outlier detection model trainer, and the XML-firewall prototype. The model trainer is responsible for inducing value-range rules for XML elements, and to train an XML classification model. It is an off-line program in the sense that it processes historical data only. The XML firewall prototype unit is an on-line program which uses the classification model, trained by the model trainer, to detect and block abnormal XML transactions.

Researchers

Prof. Yuval Elovici
elovici@bgu.ac.il

Prof. Lior Rokach
liorrk@bgu.ac.il

Prof. Bracha Shapira
bshapira@bgu.ac.il

Dr. Eitan Menahem
eitanme@bgu.ac.il

Context Aware Data Leakage Prevention for Mobile Devices

Goals

Today's smart mobile devices are able to access a variety of private data. The data may be collected by the device from its environment (e.g., via the microphone), stored in the device long term storage, or retrieved from the cloud using credentials that are stored in the device's. This valuable data may be stolen by attackers by installing a malicious application.

Protecting smartphones from data leakage is particularly important as the policy of "Bring-Your-Own-Device" gains popularity lately.

Description

The project is shared among two universities: BGU and the Technion.

An innovative and generic context-based data leakage prevention system is used to detect attempts to leak information from the device.

The system uses machine-learning techniques and learns the context in which each type of data is being sent from the device.

The context derivation is based on information that is collected by the mobile device sensors such as location and accelerometer.

Researchers

Prof. Lior Rokach
liorrk@bgu.ac.il

Dr. Asaf Shabtai
shabtaia@bgu.ac.il

Prof. Yuval Elovici
elovici@bgu.ac.il

Prof. Bracha Shapira
bshapira@bgu.ac.il

Prof. Assaf Shuster
assaf@cs.technion.ac.il

Detecting Anti-Forensic APTs

Goals

Advanced malware employ sophisticated anti-forensic techniques to evade detection by forensic instrumentation. Approximately 40% of current malware are believed to be anti-forensic.
This research aims to detect such anti-forensic malware, using non-invasive techniques.

Description

Modern malicious programs often escape dynamic analysis by detecting forensic instrumentation within their own runtime environment. This has become a major challenge for malware researchers and analysts. Current defensive analysis of anti-forensic malware often requires painstaking step-by-step manual inspection. Code obfuscation may further complicate proper analysis. Furthermore, current defensive countermeasures are usually effective only against anti-forensic techniques that have already been identified.

In this paper we propose a new method to detect and classify anti-forensic behavior, by comparing the trace-logs of the suspect program in different environments. Unlike previous works, the presented method is essentially non-invasive (does not interfere with original program flow). We separately trace the flow of instructions (Opcode) and the flow of Input-Output operations (IO). The two dimensions (Opcode and IO) complement each other to provide reliable classification. Our method can identify split behavior of suspected programs without prior knowledge of any specific anti-forensic technique; furthermore, it relieves the malware analyst from tedious step-by-step inspection. Those features are critical in the modern Cyber arena, where rootkits and Advanced Persistent Threats (APTs) are constantly adopting new sophisticated anti-forensic techniques to deceive analysis.

Researchers

Prof. Yuval Elovici
elovici@bgu.ac.il

Mordehai Guri
gurim@post.bgu.ac.il

Gabi Kedma
gabik@post.bgu.ac.il

Publications

"Non-Invasive Detection of Anti-Forensic Malware"
Malware 2013 Conference

eDare, Parts II&III

Goals

A framework for optimizing the deployment of intrusion detection systems in social networks and within the telecom infrastructure. The framework includes a variety of optimization algorithms and a network simulator. The former are used to analyze the topology of a network and suggest optimal inspection points to collect forensic data and filter out malware. The latter simulates propagation of malicious software, evaluates the effectiveness of the deployment and performs what-if analysis.

Publications

Meytal Tubi, Rami Puzis, Yuval Elovici, "Deployment of DNIDS in Social Networks", IEEE Intelligence and Security Informatics (ISI), 59-65, (2007)

Rami Puzis, Yuval Elovici, Shlomi Dolev, "Fast Algorithm for Successive Computation of Group Betweenness Centrality" Physical Review E, 76 (5): 056709, (2007)

Rami Puzis, Yuval Elovici, Shlomi Dolev, "Finding the Most Prominent Group in Complex Networks", AI Communications, 20 (4): 287-296, (2007)

Rami. Puzis, Marius David Klippel, Yuval Elovici, Shlomi Dolev, "Optimization of NIDS Placement for Protection of Intercommunicating Critical Infrastructures", EuroISI, 191 – 203, (2008)

Shlomi Dolev, Yuval Elovici, Rami Puzis, Polina Zilberman, "Incremental Deployment of Network Monitors based on Group Betweenness Centrality", IPL, 109 (20): 1172-1176, (2009)

Rami Puzis, Meytal Tubi, and Yuval Elovici, "Optimizing Targeting of Intrusion Detection Systems in Social Networks", Edt. Borko Furht – Handbook of Social Network Technologies and Applications, Springer, 549-568, (2010)

Emily Rozenshine-Kemelmakher, Rami Puzis, Ariel Felner, and Yuval Elovici, "Cost Benefit Deployment of DNIPS" IEEE ICC, 23-27, (2010)

Shlomi Dolev, Yuval Elovici, Rami Puzis, "Routing Betweenness Centrality", JACM, 57 (4): Art. 25, 1-27, (2010)

Rami Puzis, Meytal Tubi, Yuval Elovici, Chanan Glezer, and Shlomi Dolev. 2011. "A Decision Support System for Placement of Intrusion Detection and Prevention Devices in Large-Scale Networks". ACM Trans. Model. Comput. Simul. 22(1), Art. 5 (2011),

Researchers

Prof. Yuval Elovici
elovici@bgu.ac.il

Prof. Shlomi Dolev
dolev@cs.bgu.ac.il

Dr. Rami Puzis
puzis@bgu.ac.il

Patents

Rami Puzis, Shlomi Dolev, Yuval Elovici, Optimal Deployment of Infection Detection Systems over a Data Network EP 07015351.5, EP 1887744, EPO 06/010/07

Meytal Tubi, Rami Puzis, Yuval Elovici, Optimal Deployment of Infection Detection Systems over a Social Network, EP 08002999.4, EP 1990973A2, EPO 19/02/08

Rami Puzis, Shlomi Dolev, Yuval Elovici, Method for Finding the Most Prominent Group of Vertices in Complex Data Communication Networks, EP 07015351.5, EP 1887744A2, EPO 06/08/07

Data Leakage Detection in Social Networks

Researchers

Prof. Yuval Elovici
elovici@bgu.ac.il

Prof. Bracha Shapira
bshapira@bgu.ac.il

Prof. Lior Rokach
liorrk@bgu.ac.il

Prof. David Schwarz
1davidschwartz@gmail.com

Dr. Inbal Yahav
inbal.yahav@biu.ac.il

Prof. Michael Birnhack
birnhack@post.tau.ac.il

Goals

With the ever-increasing use of social networks, the amount of information exposed by users is growing at exponential rates. Such an environment leads to multiple cases of leakage (both intentional and not) of confidential information on social networks. Currently, no comprehensive solutions to this problem exist. This project is a first attempt to address this problem.

Description

This project is a collaboration between three universities – Ben-Gurion (BGU), Bar Ilan (BIU) and Tel Aviv (TAU). Each university is responsible for a different aspect of the project:

- BGU – responsible for developing the algorithms for text analysis, profile matching (identifying the same user over several social networks) and the development of a strategy for positioning the analysis tools in the social network.
- BIU – responsible for developing the crawling tools that will enable us to mine the social network and compile the dataset that will be used for the training of the model. The same software will also be used in the test phase, on "real" data.
- TAU – researching the various legal aspects and providing legal guidelines for the other two teams.

Privacy Keeper

Goals

- Improve security of smartphones in terms of data confidentiality.
- Introduce a framework for monitoring and detecting outgoing communication that might expose sensitive data about the device's owner.
- Detect unnecessary/irrelevant personal data being sent to Web-applications.

Description

Smartphone users often store confidential information on their devices. Smartphones do not provide satisfactory protection for private content and do not have any mechanisms to prevent users from providing unnecessary personal data to websites.

Our solution for detection of data leakage will be based on a combination of:

- Manual knowledge-based detection – Pre-specified rules with user's ongoing updates.
- Automatic Machine-Learning based detection – The system will detect leakage based on previous decisions and user inputs in order to minimize user interaction.
- Information automatically extracted and analyzed from the website.

The system is able to identify if a site is requesting or accessing illegitimate information. The system includes an off-line training module and an on-line analyzer. The training module is trained with sites that are analyzed by experts to approve their requests as legitimate. The analyzer is capable of distinguishing inappropriate data requests from appropriate ones. The user should be able to see the requested Web page together with security labels attached to form fields (if present) that indicate whether or not information requests are excessive or not.

Researchers

Prof. Bracha Shapira
bshapira@bgu.ac.il

Prof. Yuval Elovici
elovici@bgu.ac.il

Prof. Shlomi Dolev
dolev@cs.bgu.ac.il

Dr. Asaf Shabtai
shabtaia@bgu.ac.il

Spam Mitigation in IPv6

Researchers

Prof. Yuval Elovici
elovici@bgu.ac.il

Dr. Danny Hendler
hendlerd@cs.bgu.ac.il

Prof. Ariel Felner
felner@bgu.ac.il

Dr. Rami Puzis
puzis@bgu.ac.il

Goals

Scalable data structures for maintaining IPv6 black-, grey-, and white-lists of Spammer MTA.

Accurate heuristics for maintaining sender MTA reputation.

Detecting changes in behavior of MTAs once known as legitimate senders.

Solution

Detecting Spammers via Aggregated Historical Data Set

Maintaining blacklists as Disjoint Ranges Binary Search Tree and Buckets-Digest Bloom Filters

Results

Danny Hendler, Rami Puzis, Buckets-Digest Bloom Filters, IPO 10/02/2011

Eitan Menahem, Rami Puzis, Historical Dataset for SPAM Mitigation Using Machine Learning

Ariel Felner, Rami Puzis, Olga Brukman, Polina Zilberman, Yuval Elovici, Michael Gorelik, Disjoint Ranges Search Tree. IPO 208996, IPO 28/10/10

Identifying URLs for Black List

Goals

The following system is designed to enable the detection of malicious URLs that should be blacklisted.

In recent years, many attacks originate from surfing a malicious page on the Internet. Creating such a "black list" of malicious URLs is a goal of many companies in the industry. Surfing to a malicious URL can cause harm to the specific user and in many cases to the whole network to which the computer belongs. Categorizing a URL as malicious is not trivial for many reasons. First, in many cases the page is hiding behind a short URL that is created by some URL shortener. Second, the page looks normal but it causes the system to perform abnormally. Lastly, in many cases, the behavior of the system looks normal and therefore, by looking at a single user surfing to the malicious page, the URL cannot be detected.

Description

We first need to create a normal profile of the system. This can be done by logging the system behavior when there is no Internet connection. This stage should be done on many PCs so we can correlate and filter the normal behavior for the next stage.

In the next stage we will run a crawler; we log each page the crawler is entering and the behavior of the system during the downloading time. This is, again, done on many PCs.

The third stage should be to filter the normal behavior from the log of the second stage and to identify pages that cause abnormal behavior such as writing to unwanted places. The output of this page is a list of suspicious URLs.

The last stage would be to analyze these suspicious URLs by entering them again, but this time with a deeper analysis such as logging the written files.

The goal of this project is to be able to identify any malicious URL with zero false positives, i.e. to identify only the malicious URLs. By having a complete and accurate list, attacks that enter the system through malicious URLs can be stopped.

Many companies in the industry maintain black list of URLs. Still, none of them have a complete list. Such a list can be embedded in any Intrusion Prevention System (IPS), or even in the core of the network.

Researchers

Prof. Shlomi Dolev
dolev@cs.bgu.ac.il

Dr. Rami Puzis
puzis@bgu.ac.il

Dr. Shimrit Tzur
tzurdavi@cs.bgu.ac.il

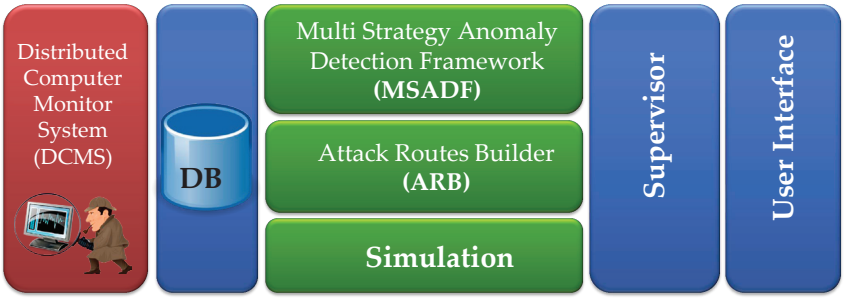
Analytics for Cyber C&C

Goals

Develop analysis plug-ins for cyber command and control platform for discovering investigation leads. Detect anomalies in process behavior and maintain file reputation.

Description

Conceptual Architecture



Validation of process behavior

1. Measure
2. Train a model
3. Test behavior
4. If anomaly conclusive, alert
5. Otherwise, analyse the error distribution

Researchers

Prof. Yuval Elovici
elovici@bgu.ac.il

Prof. Lior Rokach
liorrk@bgu.ac.il

Prof. Bracha Shapira
bshapira@bgu.ac.il

Dr. Rami Puzis
puzis@bgu.ac.il

Social Network Digestion

Goals

Enrich publicly available social network data by predicting hidden information. Find the particular information of interest by employing intelligent crawling. Actively collect hidden information via specially crafted sequences of friend requests.

Description

It is possible to gain valuable non-trivial insights into an organization's structure by clustering its social network and gathering publicly available information on the employees within each cluster.

Publications

Michael Fire, Rami Puzis , Yuval Elovici, "Organization Mining Using Online Social Networks" arXiv:1303.3741

Zahy Bnaya, Rami Puzis, Roni Stern, Ariel Felner, Balancing Exploration and Exploitation in Social Network Queries, ASE Human Journal, ISBN: 978-1-62561-004-1 (forthcoming)

Michael Fire, Gilad Katz, Lior Rokach, Yuval Elovici, "Link Reconstruction Attack using Link Prediction Algorithm to Compromise Social Network Privacy", Security & Privacy in Social Networks

Michael Fire, Lena Tenenboim-Chekina, Rami Puzis, Ofrit Lesser, Lior Rokach, Yuval Elovici, "Computationally Efficient Link Prediction in Variety of Social Networks", to appear in ACM Transactions on Intelligent Systems and Technology, 5(1), (2014)

Aviad Elishar, Michael Fire, Dima Kagan, and Yuval Elovici, Homing "Socialbots: Intrusion on a Specific Organization's Employee using Socialbots", SNAA 2013

Zahy Bnaya, Rami Puzis, Roni Stern, Ariel Felner, "Bandit Algorithms for Social Network Queries," ASE/IEEE SocialCom, (2013)

Roni Stern, Liron Smama, Rami Puzis, Tal Beja, Zahy Bnaya, and Ariel Felner, "TONIC: Target Oriented Network Intelligence Collection for the Social Web", In AAAI-13, Bellevue, Washington, USA, and in BISFAI 2013 (2013)

Zahy Bnaya, Rami Puzis, Roni Stern, and Ariel Felner, "Volatile Multi-Armed Bandits for Guaranteed Targeted Social Crawling", In AAAI-13, Bellevue, Washington, USA, (2013)

Puzis, R., Bakulin, Y., Elovici, Y., Glezer, C. "Targeted Marketing in Social Networks," In Proc. 6th Israeli IE&M Research Conference, Ma'ale-Hahamisha, March 17-18, 2013

Researchers

Prof. Yuval Elovici
elovici@bgu.ac.il

Dr. Rami Puzis
puzis@bgu.ac.il

Mr. Michael Fire
mickyfi@post.bgu.ac.il

Self-stabilizing Hypervisor

Researchers

Prof. Shlomi Dolev
dolev@cs.bgu.ac.il

Dr. Alex Binun
Mr. Mark Block
Mr. Martin Kahil
Dr. Marc Lacoste
Mr. Boaz Minuchin
Mr. Zeev Vaxman Fisher
Dr. Aurélien Wailly
Dr. Reuven Yagel

Goals

The main goal is to have a robust self-stabilizing cloud. A cloud with this feature will need far less human intervention to be functional, and the recovery from attacks will be much quicker.

The intermediate goal is to have a self-stabilizing hypervisor that ensures correctness of each VM and protects it from the existence of potential Byzantine neighboring VMs.

Description

The system is a self-stabilizing hypervisor (virtualization tool) that will be robust in the presence of transient faults in VMs and Byzantine VMs.

The cloud is becoming more and more popular, and thus the need for resource utilization. All cloud providers known to us use virtualization to achieve good utilization of resources, and to provide privacy to each client. Nonetheless security remains a major issue, since VMs may break out of the virtual environment and take over the actual host. So to provide security and to meet SLAs, an automatically recovering system of virtual machines is a great contribution to the field.

Currently a self-stabilizing architecture for the KVM hypervisor has been composed, and code implementation has just started. We expect iterative model refinement according to the challenges that will occur during development. After having a self-stabilizing KVM version that runs on one machine we are planning to implement this on multiple machines.

The research could save a lot of money and human interaction while managing a cloud. In addition the automatic recovery from transient faults and attacks will make it more feasible to meet certain SLAs.

Deterring Attacks Against Critical IT Infrastructure

Goals

In our previous work the notion of arbitrators in a Peer-to-Peer (P2P) network was used to enforce the client-server agreement for the limited case of conditional anonymity. Arbitrators are P2P semi-trusted entities that function as a jury in the technology court of law. The communicating parties, users and servers, agree in the initial phase on a set of arbitrators that they trust (reputation systems may support their choice). Then, the user divides its identity into shares and sends each share to one arbitrator, such that only a large enough number of arbitrators can reveal the identity of the user. The CA signs the shares that the user distributes to the arbitrators, vouching for their authenticity. The communication between the user and the server is performed in an undeniable manner, which means that the server can convince the arbitrators that the user misbehaved. In the event that the server finds a violation of the terms of the policy, the server proves to the arbitrators that a violation took place and the arbitrators reconstruct the user's identity.

An important objective of this research is construction of schemes that encourage commitment to a policy and enforcement of this commitment, even without a third party. In this approach, a client commits to a certain policy or agreement and in return receives service from a server. The client's commitment includes hidden information such as the client's identity or a signed financial instrument such as a check or a bond. If the client breaches the terms of the agreement then the server can expose the hidden information without assistance from external parties, such as arbitrators.

Description

Attacking critical IT infrastructure is almost always risk-free. Whether targeting government services or financial institutions, an attacker can sit in the comfort and safety of his home and mount one attack after the other. Protected from identification by the virtual anonymity of the Internet and from legal proceedings by being in a different jurisdiction than the target, the greatest risk for most attackers is that their attack may fail.

The technology can be used in critical IT infrastructures as another cyber security measure.

Researchers

Mr. Dan Brownstein
danbr@cs.bgu.ac.il

Prof. Shlomi Dolev
dolev@cs.bgu.ac.il

Dr. Niv Gilboa
gilboan@bgu.ac.il

Results

Development is in progress. Several algorithms are needed for developing the protocol of which only a few are already constructed. Among these algorithms are: construction of a small DFA that verifies signatures, construction of an efficient scheme for functional encryption for Cascade Mealy Machine (extension of the currently known functional encryption schemes for regular languages). In addition, there is a team of fourth year Communication Systems Engineering students who implement the scheme.

Securing MapReduce Computations using Accumulating Automata

Goals

MapReduce is a programming model that was introduced by Google in 2004 for large-scale data processing. MapReduce also has extensive applications for cloud computing. The use of public, private, hybrid, and multi-clouds gives rise to several challenges regarding security and data management. Companies and countries each have their own regulations for using the clouds.

Description

Various challenges in the hybrid clouds, e.g., malicious mappers, malicious reducers, non-secure communications between the map and the reduce phases, are still not being considered. These challenges could reveal data or computations in the clouds. We explore a secure model for MapReduce computations that will provide a solution to the aforementioned problems.

State-transition systems are accumulating automata, $A = (V, \Sigma, T)$, where V is a set of nodes, Σ is an input data split, and T is a transition function. Each node has a value, and these values are shared among several mappers using secret sharing.

A secure version of MapReduce computations using accumulating automata solves multiple real world problems, where users do not want to reveal data and computations in the cloud. A few examples include: accessing the patients' database to enhance the drugs and diseases relation without revealing the patients' information; shopping a website's database to enhance advertisement policies without revealing customers' information; and computations on a bank database without revealing individuals' information and illustrate the need for secure MapReduce using accumulating automata.

Researchers

Prof. Shlomi Dolev
dolev@cs.bgu.ac.il

Shantanu Sharma
sharmas@cs.bgu.ac.il

Succinct Big Data Representations

Goals

Given a large set of measurement data, in order to identify a simple function that captures the essence of the data, we suggest representing the data by an abstract function, in particular by polynomials.

We manipulate the datapoints to achieve interpolation, extrapolation and dynamic representation of the data. Those objectives are challenging, since in practice the data can be noisy and even Byzantine, where the Byzantine data represents an adversarial value that is not limited to being close to the correct measured data.

In the world of big data, traditional security technologies lack the sophisticated capabilities required to detect and protect against advanced persistent threats, fraud, and insider attacks. Our approach of representing the big data in an abstract fashion advanced the goal of identified and discarded anomalies or out-layers in the data in a constructive manner.

Description

Consider the task of representing information in an error-tolerant way, such that it can be formulated even if it contains noise or even if the data are partially corrupted and destroyed. Our research offers the concept of data interpolation in data aggregation and representation, as well as the new big data challenge, where abstraction of the data is essential in order to understand the semantics and usefulness of the data.

Development Stage and Development Status-Summary

For the interpolation task, we present two solutions, one that extends the Welch-Berlekamp technique in the case of multidimensional data, and copes with discrete noise and Byzantine data, and the other based on Arora and Khot techniques, extending them in the case of multidimensional noisy and Byzantine data.

Further research includes prediction of the data trends based on the periodic behavior of the input and extrapolating the data at Fourier's domain, where the Byzantine data (e.g., anomalies or out-layers) is identified and discarded.

In addition, we suggest handling the dynamic change of the data using property testing.

Researchers

Hadassa Daltrophe
hd@cs.bgu.ac.il

Prof. Shlomi Dolev
dolev@cs.bgu.ac.il

Dr. Zvi Lotker
zvilo@bgu.ac.il

Detecting Intruders Using Active Network Probing

Researchers

Prof. Yuval Elovici
elovici@bgu.ac.il

Prof. Lior Rokach
liorrk@bgu.ac.il

Prof. Bracha Shapira
bshapira@bgu.ac.il

Dr. Eitan Menahem
eitanme@bgu.ac.il

Publications

Eitan Menahem, Yuval Elovici, Nir Amar, and Gabi Nakibly. 2013. ACTIDS: an "active strategy for detecting and localizing network attacks." Proceedings of the 2013 ACM workshop on Artificial intelligence and security (AISec '13).

Goals

Detect and localize network-wide attacks, which have the potential of degrading the network quality of service. Such attacks include, among others, attacks against the routing protocols (e.g., OSPF) and against the domain name service (DNS). In this project, we implemented an innovative IDS solution in a network simulation (omnet++), and researched a new multi-inducer anomaly detection scheme.

Description

We researched a new detection mechanism, ACTIDS (Active Intrusion Detection System) that, given a network-topology, automatically computes a probing scheme to cover the network with periodical Probe-Packets. The probes traverse the network and record the network's quality of service. Next, ACTIDS apply multiple machine-learning techniques (one-class learning) to detect network anomalies on the information extracted from the Probe-Packets.

Next, we implemented the ACTIDS framework in a network emulation (GNS3), which allowed us to evaluate the framework in a very realistic environment. The emulated network included the actual code of many real hardware devices, such as routers and switches.

An Independent Vehicle Authentication Using Non-Fixed Attributes

Goals

We present a vehicle authentication approach that utilizes the out-of-band verification of dynamic and sense-able attributes of the vehicle.

Authentication is an important issue regarding vehicle network security. Vehicles communicate through wireless channels and need to verify the peer vehicle identity, before exchanging sensitive information. If a vehicle assumes a fake identity and transmits bogus messages to peer vehicles, it could turn into a life-threatening situation.

Description

Vehicles can authenticate peer vehicles using a certificate from a trusted certificate authority. However, besides the certificate verification, an online authenticity proof is also required. In our previous work, we suggested out-of-band fixed attribute verification of a vehicle against the certified attributes from a trusted certificate authority. The coupling between the certified public key and the sense-able static attributes confirms the vehicle authenticity. There is a scenario in which an impersonation attack is successful, in spite of the out-of-band fixed sense-able attribute verification. Therefore, we suggest coupling the non-fixed sense-able attributes and the session secret of the vehicle. It ensures a unique identity for every vehicle and resolves the active impersonation attack, i.e. man-in-the-middle attack.

Modern vehicles are equipped with Global Positioning System (GPS), sensors, actuators, electronic control and processing units. Moreover, a camera, laser beam source and autocollimator mounted on the vehicle can observe the static as well as dynamic attributes of the peer vehicle. Therefore, it is feasible to implement the proposed approach without any roadside infrastructure available, and only vehicle customization is required.

All major automotive giants such as BMW, Toyota, GM, Nissan, Bosch, Delphi are customizing their vehicles for these real world applications. For example, GM has OnStar service in their vehicles which utilizes the cellular infrastructure for driver assistance, road navigation, vehicle repair, theft detection, etc.

Researchers

Prof. Shlomi Dolev
dolev@cs.bgu.ac.il

Nisha Panwar
panwar@cs.bgu.ac.il

Prof. Michael Segal
segal@cse.bgu.ac.il

Cyber Spark The Ecosystem

The Israeli Cyber Innovation Arena in the Negev

Drawn by BGU with its proven expertise, the State of Israel and the Israel Defense Forces are turning Beer-Sheva into the country's cyber capital. Thousands of soldiers and officers from elite telecommunications and intelligence units, together with key national cyber bureaus, are being relocated to Beer-Sheva to leverage the University's education and research environment while working with the industrial giants that have invested in the burgeoning ecosystem in Beer-Sheva.

Contact for more Information:
Zafrir Levy, Vice President
Business Development
Exact Sciences & Engineering
BGN Technologies
cyber@bgu.ac.il | Tel: +972-52-256-5715

Ben-Gurion University of the Negev aspires to fulfill the vision of Israel's first prime minister, David Ben-Gurion, who believed that Israel's future lay in the development of the Negev, a desert area comprising more than sixty percent of the country. Today, at its campuses in Beer-Sheva, Sede Boqer and Eilat, close to 20,000 students are enrolled in the Faculties of Engineering Sciences, Health Sciences, Natural Sciences, Humanities and Social Sciences and the Guilford Glazer Faculty of Business and Management, the Joyce and Irving Goldman Medical School and the Kreitman School of Advanced Graduate Studies. Major University research institutes include the National Institute for Biotechnology in the Negev, the Jacob Blaustein Institutes for Desert Research with the Albert Katz International School for Desert Studies, the Ilse Katz Institute for Nanoscale Science and Technology and the Ben-Gurion Research Institute for the Study of Israel and Zionism. Repeatedly voted the most popular choice of Israeli undergraduate students, the University is known for its dynamic atmosphere and commitment to excellence in teaching and research.

Ben-Gurion University is a world leader in arid zone research, offering its expertise to many developing countries. In keeping with its mandate, it plays a key role in promoting industry, agriculture and education in the Negev. Thousands of its students take part in community-oriented activities and special tutoring projects. The University welcomes exciting challenges in innovative fields of research and strives to bring new opportunities to Beer-Sheva and the Negev while continuing its pursuit of academic excellence and expanding its contribution to the community.

אוניברסיטת בן-גוריון בנגב
Ben-Gurion University of the Negev