

At the Center of Innovation

CYBER

@ BGU

Spotlight on  
Excellence  
in Research





EMC

RSA

BGN

ORACLE

Allscripts™

אוניברסיטת בן-גוריון בנגב





# CYBER

# @BGU

## Spotlight on Excellence in Research

- 4 Defense against Covert Channel Cyber Attack Over Video Stream Payload
- 5 Scalable Attack Path Finding for Increased Security
- 6 Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection
- 7 Replacing Byzantine Participants
- 8 Creation and Management of Social Network Honeypots for Detecting Targeted Cyber Attacks
- 9 Runtime Execution Introspection for Security Protection Using Machine Learning
- 10 Fake News Detection Using Topic Authenticity
- 11 Advanced Analytics for Connected Cars Cyber Security
- 12 Detection of Malicious Webmail Attachments Based on Propagation Patterns
- 13 AntiBotics: Ransomware Prevention Using Application Authentication-based File Access Control
- 14 Secret Double Octopus
- 15 Succinct Big Data Representations for Privacy and Efficiency
- 16 CloTA: Collaborative Anomaly Detection via Blockchain
- 17 Deterring Attacks against Critical IT Infrastructure
- 18 Securing MapReduce Computations Using Accumulating Automata
- 19 DROPWAT: An Invisible Network Flow Watermark for Data Exfiltration Traceback
- 20 Network Flow Watermarking: A Survey
- 21 INFLOW: Inverse Network Flow Watermarking for Detecting Hidden Servers
- 22 When Replacement Smartphone Components Attack
- 23 A Lightweight Vulnerability Mitigation Framework for IoT Devices
- 24 Customer Data Leakage Prevention
- 25 Handwritten Signature Verification Using Hand Worn Devices
- 26 Independent Vehicle Authentication Using Non-fixed Attributes
- 27 Know Your Enemy: Characteristics of Cyber Attacks on Medical Imaging Devices
- 28 Context-based Data Leakage Detection
- 29 Cyber-Med: Risk Assessment and Practical Detection Methodology of Cyber Attacks Aimed at Medical Device Ecosystems
- 30 Self-Stabilizing Cloud Infrastructure
- 31 Activity-based Verification Continuous User Verification after Successful Login
- 32 Oops!.. I Think I Scanned a Malware
- 33 Socialbots Studies
- 34 Taxonomy of Mobile Users' Security Awareness
- 35 Game of Drones: Detecting Streamed POI from Encrypted FPV Channel
- 36 VisiSploit: An Optical Covert-channel to Leak Data through an Air-gap
- 37 LED-it-GO: Leaking (a lot of) Data from Air-gapped Computers via the (small) Hard Drive LED
- 38 Identifying URLs for Blacklist
- 39 Data Leakage Detection in Social Networks
- 40 Detecting Anti-Forensic APTs
- 41 SecretSkyDB
- 42 Personal Information Leakage through Online Social Networking: Leakage Prevention and Leakers Detection
- 43 Generic Black-Box End-to-End Attack against RNNs and Other API Call-based Malware
- 44 Context Aware Data Leakage Prevention for Mobile Devices
- 45 USBee: Air-gap Covert-channel via Electromagnetic Emission from USB
- 46 Acoustic Data Exfiltration from Speakerless Air-gapped Computers via Covert Hard Drive Noise ('DiskFiltration')
- 47 Social Network Digestion
- 48 Unknown Malware Detection Using Network Flow Pattern Classification
- 49 Fansmitter: Acoustic Data Exfiltration from (Speakerless) Air-gapped Computers
- 50 GSMem: Data Exfiltration from Air-gapped Computers over GSM Frequencies
- 51 Bitwhisper: Covert Signaling Channel Between Air-gapped Computers Using Thermal Manipulations
- 52 AirHopper: Bridging the Air-gap Between Isolated Networks and Mobile Phones Using Radio Frequencies
- 53 xLED: Covert Data Exfiltration from Air-gapped Networks via Router LEDs
- 54 aIR-Jumper: Covert Air-gap Exfiltration/Infiltration via Security Cameras & Infrared

# Defense Against Covert Channel Cyber-attack Over Video Stream Payload

## Researchers

Prof. Ofer Hadar  
hadar@bgu.ac.il

Yoram Segal  
yoramse@post.bgu.ac.il

## Publications

R. Dubin, A. Dvir, O. Pele and O. Hadar, "I know what you saw last minute: Encrypted HTTP adaptive video streaming title classification," IEEE Transactions on Information Forensics & Security, Vol. 12, No. 12, pp. 3039-3049, 2017.

R. Segal, R. Birman, E. Hadas and O. Hadar, "Defense from covert channel cyber attack over video stream payload," RESCUE 2017 workshop, 22nd IEEE European Test Symposium, Limassol, 2017.

R. Segal, E. Segal and O. Hadar, "Cyber attack/defense based on estimated motion vectors via covered channel," TRUDEVICE Workshop Barcelona, 2016.

R. Dubin, A. Dvir, O. Pele, and O. Hadar, "I Know what you saw last minute: The Chrome browser case," Blackhat Europe 2016, London, 2016.

Y. Amsalem, A. Poznov. A. Bedinerman, M. Kotcher, and O. Hadar, "Cyber attack/defense algorithms based on data hiding in compressed video stream," SPIE Optics + Photonics Conference, San Diego, 2015.

## Goals

Video streaming and image downloading account for 50% of Internet traffic today, a figure which is expected to rise to 67% of Web traffic by 2020. These attack routes provide a lot of space to implant malicious code (the image size and video bitrate may reach tens of megabits). Moreover, such covert channels do not utilize the computer's legitimate data transfer system and malware detection systems, enabling attackers to transfer data while evading detection. This research is aimed at investigating this attack model and developing countermeasures against this growing threat.

## Description

In this project, researchers showed how the video compression domain can be used as a "backdoor" for cyber-attacks. In addition to demonstrating how to establish this channel, researchers showed the ease with which video streams can be used as a vehicle for passing sequences of commands and performing malicious actions remotely on a targeted computer; more specifically, they were able to create a covert channel with sufficient bandwidth to allow them to remotely control the computer without compromising the quality of the video stream. They also demonstrated how an attacker can exploit the estimated motion vector in the ubiquitous H.264 video stream. This can be done via proxies in near real-time with a limited amount of CPU consumption. The attack was demonstrated on several different platforms to show that the security breach is not hardware dependent.

Having shown the feasibility of this attack model, the researchers are now focusing on developing countermeasures. Their proposed Coucou solution, is based on advanced techniques aimed at providing a comprehensive solution against attacks conducted over video streams via covert channels. The techniques under development leverage the attack model and work on the frequency domain and motion vectors, without decreasing runtime or compromising image quality. The researchers are pursuing local solutions (the proposed technique is based on inserting random noise into the stream and allows the client to choose his/her protection level. Network and system solutions are also being considered, including a technique that involves changing and increasing the standard of compression to add a digital signature to the video stream.



# Scalable Attack Path Finding for Increased Security

## Researchers

Tom Gonda  
tom.gonda@gmail.com

Prof. Bracha Shapira  
bshapira@bgu.ac.il

Dr. Rami Puzis  
puzis@bgu.ac.il

## Publications

T. Gonda, R. Puzis, and B. Shapira, "Scalable Attack Path Finding for Increased Security," International Conference on Cyber Security Cryptography and Machine Learning [CSCML], 2017, 234-249.

T. Gonda, G. Shani, R. Puzis, B. Shapira, "Ranking Vulnerability Fixes Using Planning Graph Analysis," IWAISe-17, 2017.

## Goals

Software vulnerabilities can be leveraged by attackers to gain control of a host. Attackers can then use the controlled hosts as stepping stones for compromising other hosts until they create a path to the critical assets. Consequently, network administrators must examine the protected network as a whole rather than each vulnerable host independently. In recent years, logical attack graphs are used to find the most critical vulnerabilities and devise efficient hardening strategies for organizational networks. Most techniques for ranking vulnerabilities either do not scale well to medium-large networks with hundreds or thousands of hosts. (e.g. brute-force attack plan enumeration), or are not well suited for the analysis of logical attack graphs (e.g. centrality measures). Research is focused on improving the run time of cyberattack modeling tools.

## Description

One solution explored by the researchers is reducing the graph representing the attacker steps. The reductions allow security admins to analyze bigger networks with complex attacker logic by simplifying the task of searching and eliminating optimal attacker paths. Results on an attack graph extracted from a network of a real organization with more than 300 hosts and 2400 vulnerabilities show that using the proposed graph reductions can improve the search time by a factor of 4 while maintaining the quality of the results.

In another solution, they suggest an analysis of the planning graph (from classical planning) derived from the logical attack graph to improve the accuracy of centrality-based vulnerability ranking metrics. The planning graph also allows efficient enumeration of the set of possible attack plans that use a given vulnerability on a specific machine. For this, they propose a set of centrality-based heuristics for reducing the number of attack plans and comparisons with previous vulnerability ranking metrics. Results show that metrics computed over the planning graph are superior to metrics computed over the logical attack graph or the network connectivity graph.

# Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection

## Researchers

Yisroel Mirsky  
yisroel@post.bgu.ac.il

Tomer Doitshman  
tomerdo@post.bgu.ac.il

Prof. Yuval Elovici  
elovici@inter.net.il

Dr. Asaf Shabtai  
shabtaia@bgu.ac.il

## Publications

Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection," Network and Distributed System Security Symposium [NDSS'18], 2018.

## Goals

Neural networks have become an increasingly popular solution for network intrusion detection systems (NIDS). Their capability to learn complex patterns and behaviors make them a suitable solution for differentiating between normal traffic and network attacks. However, a major drawback of neural networks is the amount of resources needed to train them. Many network gateways and routers devices, which could potentially host an NIDS, simply do not have the memory or processing power to train and sometimes even execute such models. More importantly, the existing neural network solutions are trained in a supervised manner, meaning that an expert must label the network traffic and update the model manually. In response to this problem, the researchers have developed Kitsune: a plug and play NIDS which can learn to detect attacks on the local network, without supervision, and in an efficient online manner.

## Description

Kitsune's core algorithm (KitNET) uses an ensemble of neural networks called autoencoders to collectively differentiate between normal and abnormal traffic patterns. KitNET is supported by a feature extraction framework which efficiently tracks the patterns of every network channel. The evaluations show that Kitsune can detect various attacks with a performance comparable to offline anomaly detectors, even on a Raspberry Pi. This demonstrates that Kitsune can be a practical and economic NIDS.





# Replacing Byzantine Participants

## Researchers

Prof. Shlomi Dolev  
shlomidolev@gmail.com

Amitay Shaer  
shaera@post.bgu.ac.il

Prof. Roberto Baldoni [Cyber Security Czar of Italy]  
baldoni@dis.uniroma1.it

Dr. Silvia Bonomi  
bonomi@dis.uniroma1.it

## Publications

S. Dolev, A. Shaer, R. Baldoni, and S. Bonomi, "Replacing Byzantine Participants," International Symposium on Cyber Security Cryptography and Machine Learning, 2017.

## Goals

Detect two-faced malicious processes during distributed agreement, and kill and replace malicious participants while keeping the process time efficient.

## Description

We suggest various ways for detection of Byzantine processes, i.e., processes which deviate from the protocol in an arbitrary way. Detection can be accomplished by comparing the (black boxed) result of the Byzantine consensus on each of the processes gossiped input, and then comparing these gossiped messages with the decision value of the consensus on the particular input.

We adopted a new approach to eliminating the Byzantine processes: Suppose several processes report another process as faulty, in this case, all the reporting processes will be killed unless enough reporting processes exist.

To address this issue, we suggest a protocol composed of fast and slow parts. At first, all processes are assumed to be correct and the protocol starts with the fast algorithm. As long as there is no indication of a Byzantine activity, the fast algorithm continues to work. The moment an indication of Byzantine activity has been discovered, the processes start to execute the slow algorithm and the two-faced processes are thus eliminated.

### Researchers

Abigail Paradise  
abigailparadise@gmail.com

Dr. Asaf Shabtai  
shabtaia@bgu.ac.il

Dr. Rami Puzis  
puzis@bgu.ac.il

Aviad Elyashar  
aviade@post.bgu.ac.il

Prof. Yuval Elovici  
elovici@inter.net.il

Dr. Mehran Roshandel  
Mehran.Roshandel@telekom.de

Dr. Christoph Peylo  
Christoph.Peylo@telekom.de

### Publications

A. Paradise, R. Puzis, A. Elyashar, Y. Elovici, and A. Shabtai, "Creation and Management of Social Network Honeypots for Detecting Targeted Cyber Attacks." IEEE Transactions on Computational Social Systems [IEEE T-CSS], 2017.

# Creation and Management of Social Network Honeypots for Detecting Targeted Cyber Attacks

## Goals

Reconnaissance is the initial and essential phase of a successful advanced persistent threat (APT). In many cases attackers collect reconnaissance information from social media, such as professional social networks. This information is used to select members that can be exploited to penetrate the organization. Detecting such malicious reconnaissance activity is extremely hard because it is performed outside the organization premises.

## Description

The researchers propose a framework for management of social network honeypots to aid in detection of APTs at the reconnaissance phase. Using a field trial conducted with the cooperation of a large European organization, they analyzed the deployment process of the social network honeypots and their maintenance in real social networks. The honeypot profiles were successfully assimilated into the organizational social network and received suspicious friend requests and mail messages that revealed basic indications of a potential forthcoming attack.

The project also includes exploring the behavior of employees in professional social networks, their resilience and vulnerability toward social network infiltration.





# Runtime Execution Introspection for Security Protection Using Machine Learning

## Researchers

Prof. Shlomi Dolev  
shlomidolev@gmail.com

Mohammad Ghanayim  
ghanayim@post.bgu.ac.il

Dr. Alexander Binun  
binun@cs.bgu.ac.il

Dr. Sergey Frenkel  
sfergei51@gmail.com

Prof. Yeali S. Sun  
sunny@ntu.edu.tw

## Publications

S. Dolev, M. Ghanayim, A. Binun, S. Frenkel and Y. S. Sun, "Relationship of Jaccard and Edit Distance in Malware Clustering and Online Identification," IEEE International Symposium on Network Computing and Applications, NCA, 2017.

## Goals

The goal of this project is to learn and analyze the behavior of labeled traces of API calls and build classifiers based on that analysis to be executed in hypervisor environments in order to detect intrusions and threats.

## Description

This research is part of a joint project with Prof. Sun from National Taiwan University, funded by the Israeli Ministry of Science and the Taiwanese National Science Council. We used machine learning to perform behavioral analysis and classification of malwares, based on traces of their calls to OS APIs; we first trained a classifier by clustering data consisting only of malicious API call traces, based on the Jaccard index. Then, during the prediction phase, a query trace is labeled as either benign or malicious by its distance or similarity from the medoids of the clusters, (i.e., a query trace is labeled as benign if and only if it is anomalous to all clusters), which proved to be 90% accurate in our experiments. To perform efficient clustering, we resorted to techniques used in data mining, while keeping our solution platform-independent by disregarding the semantics of API names and arguments. Similar traces were grouped together by a method of Locality Sensitive Hashing, which maps similar items together by hashing them several times, avoiding the costly explicit computation of their pairwise similarity. Math-wise, we relied on the linear time Jaccard index to achieve lower and upper bounds on the more accurate quadratic time Edit Distance; these bounds were then used to approximate the Normalized Edit Distance based on the Jaccard index. The latter approximation is utilized for refinement of the clustering, which was originally done with respect to Jaccard. In particular we were able to use the efficient Jaccard index to gain the accurate, yet time consuming, Edit Distance.



# Fake News Detection Using Topic Authenticity

## Description

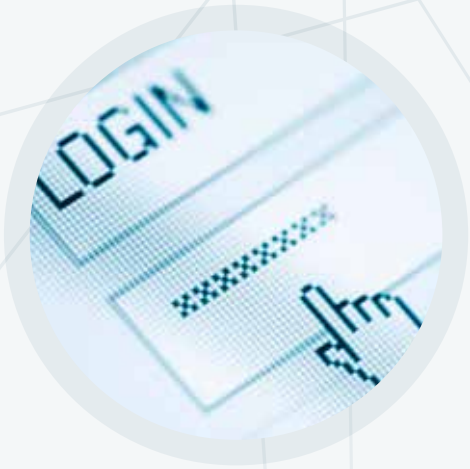
Researchers propose an approach for the detection of fake news in online social media (OSM). The approach is based on the authenticity of online discussions published by fake news promoters and legitimate accounts. Authenticity is quantified using a machine learning (ML) classifier that distinguishes between fake news promoters and legitimate accounts. They also propose novel link prediction features that were shown to be useful for classification. These include processes used to divide the dataset into categories representing topics or online discussions and measuring the authenticity of online discussions is provided. Using new data collection methods for OSM, they retrieved accounts and their posts in order to train traditional ML classifier, and developed guidelines for manually labeling accounts. The proposed approach is demonstrated using a Twitter pro-ISIS fanboy dataset provided by Kaggle. The results show that this method can successfully distinguish between the false “authenticity” from fake news promoters, and legitimate accounts. Thus, the suggested approach is effective for discriminating between topics that were strongly promoted by fake news promoters and those that attracted authentic public interest.

### Researchers

Aviad Elyashar  
aviad.elishar@gmail.com

Jorge Bendahan  
jorgeaug@post.bgu.ac.il

Dr. Rami Puzis  
puzis@bgu.ac.il



# Advanced Analytics for Connected Cars Cyber Security

## Researchers

Matan Levi  
matanle@post.bgu.ac.il

Dr. Yair Allouche  
YAIR@il.ibm.com

Prof. Aryeh Kontorovich  
karyeh@cs.bgu.ac.il

## Publications

M. Levi, Y. allouche, and A. Kontorovich, "Advanced Analytics for Connected Cars Cyber Security," IEEE 87th Vehicular Technology Conference, Porto, 2018.

## Goals

As modern vehicles become more connected, they also become much more vulnerable to cyber-attacks. Researchers from BGU and IBM are working on a machine learning approach to protect connected vehicles (fleets and individuals) against such attacks.

## Description

The machine learning system monitors different vehicle interfaces (Network, CAN and OS), extracts relevant information based on configurable rules and sends it to a trained generative model to detect deviations from normal behavior. Using a configurable data collector, it provides a higher level of data abstraction as the model is trained based on events instead of raw data, which has a noise-filtering effect and eliminates the need to retrain the model whenever a protocol changes. The adaptive thresholds method detects sophisticated and realistic anomalies, which are missed by other existing methods monitoring the CAN bus only, and scales efficiently from monitoring individual cars to serving large fleets.





# Detection of Malicious Webmail Attachments Based on Propagation Patterns

## **Researchers**

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

Yehonatan Cohen  
yehonatc@gmail.com

Amir Rubin  
amirubin87@gmail.com

## **Publications**

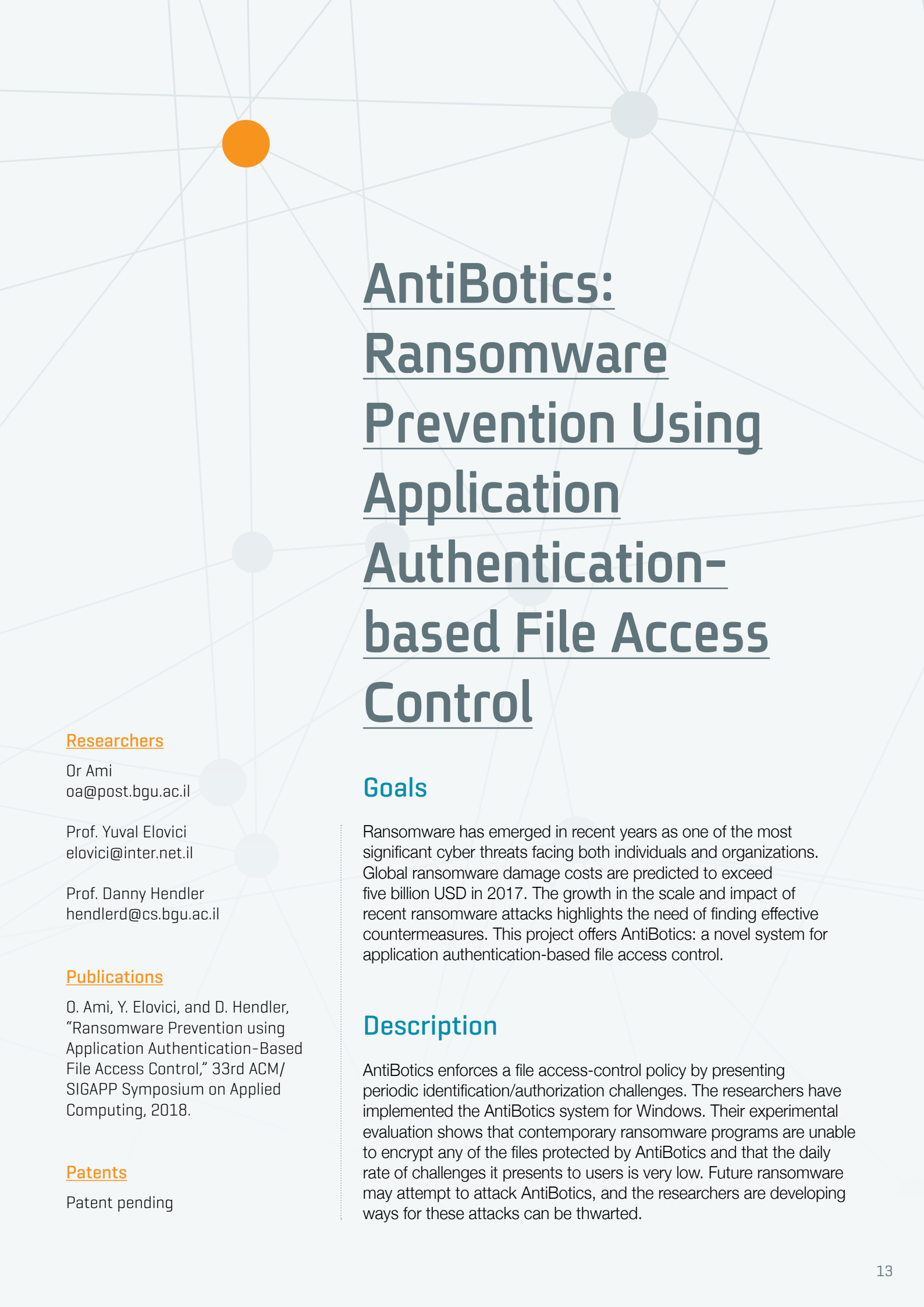
Y. Cohen, D. Hendler, and A. Rubin, "Detection of malicious webmail attachments based on propagation patterns," Knowledge-Based Systems Journal 141: 67-79, 2018.

## **Goals**

Email remains one of the key media used by cybercriminals for distributing malware. Based on a large data set consisting of antivirus telemetry reports, the researchers conducted the first comprehensive study of the properties of malicious webmail attachments and were able to distinguish the general web-borne malware population in terms of the reach, type and family.

## **Description**

The study demonstrated that there are distinctions among the general web-borne malware population in terms of the malware reach (the number of machines to which the malware is downloaded), malware type and family. Researchers also found that malicious webmail attachments are unique in the manner in which they propagate through the network. These findings were leveraged to define features of malware propagation patterns. These features are derived from a time-series representation of malware download rates and from the community structure of graphs that model the network paths through which malware propagates. Based on these features, they developed a high-quality detector for webmail attachments.



# AntiBotics: Ransomware Prevention Using Application Authentication- based File Access Control

## Researchers

Or Ami  
oa@post.bgu.ac.il

Prof. Yuval Elovici  
elovici@inter.net.il

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

## Publications

O. Ami, Y. Elovici, and D. Hendler,  
“Ransomware Prevention using  
Application Authentication-Based  
File Access Control,” 33rd ACM/  
SIGAPP Symposium on Applied  
Computing, 2018.

## Patents

Patent pending

## Goals

Ransomware has emerged in recent years as one of the most significant cyber threats facing both individuals and organizations. Global ransomware damage costs are predicted to exceed five billion USD in 2017. The growth in the scale and impact of recent ransomware attacks highlights the need of finding effective countermeasures. This project offers AntiBotics: a novel system for application authentication-based file access control.

## Description

AntiBotics enforces a file access-control policy by presenting periodic identification/authorization challenges. The researchers have implemented the AntiBotics system for Windows. Their experimental evaluation shows that contemporary ransomware programs are unable to encrypt any of the files protected by AntiBotics and that the daily rate of challenges it presents to users is very low. Future ransomware may attempt to attack AntiBotics, and the researchers are developing ways for these attacks can be thwarted.



# Secret Double Octopus

## Researchers

Prof. Shlomi Dolev  
shlomidolev@gmail.com

Dr. Shimrit Tzur-David  
Shimritd@doubleoctopus.com

## Results

An authentication product is developed as a startup company in collaboration with JVP Cyber Labs. Several patents have been assigned to Secret Double Octopus.

## Goals

Next generation internet security using innovative authentication schemes.

## Description

Secret Double Octopus grew out of Prof. Dolev's research group's activities at the Dept. of Computer Science. When postdoc Dr. Tzur-David joined the group with her interest in software defined networks (SDN), she was exposed to the group's work on multi-physical channels transmission and secret sharing; it was natural to go ahead and design multi-physical channels, secret sharing SDN.

Eventually, Prof. Dolev suggested the authentication schemes that form the Overlay Security concept that is at the heart of Secret Double Octopus technology. The Overlay Security concept is not necessarily tied to software defined networks, or to secret sharing, or to different physical routes. It is based on the security of existing protocols over (possibly) the same physical network and is the key innovative concept in the DNA of Secret Double Octopus technology. The idea is to use the combined security, authenticity and identification of existing logical channels - such as messengers, emails, push tokens - by using them in parallel, so hackers need to break them all to reveal the information sent. This novel concept is being used in the first password free authentication product of Secret Double Octopus and can certainly serve as the concept for the future quantum safe Internet.



# Succinct Big Data Representations for Privacy and Efficiency

## Researchers

Prof. Shlomi Dolev  
shlomidolev@gmail.com

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

Philip Derbeko  
philip.derbeko@gmail.com

Prof. Jeffrey Ullman  
ULLMAN@CS.stanford.edu

## Development Stage and Status

Current research is focused on building a model for statistical queries with wavelets and polynomials that keep the data in privacy-preserving way.

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.

## Goals

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

The researchers are developing a means of creating a succinct, similitude representation of the data, such that it allows for statistical calculations and also preserves privacy of the data. This dramatically reduces the effects of data breaches and also makes it easier to keep the data safe. The data cannot be breached if it is not there to begin with! These methods are especially valuable when applied to IOT devices, where it saves power, protects storage and networks and keeps the data more secure.

## Description

The proposed methods vary with the type and the target queries, and include capturing the essence of the data by abstract function, such as wavelets and polynomials and using controlled sampling to build a compact representation of the data with bounded error. The researchers process the data points to build a model for 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.



# CloTA: Collaborative Anomaly Detection via Blockchain

## Description

With their rapid growth and deployment, Internet of things (IoT) devices have become a central aspect of our daily lives. However, they tend to have many vulnerabilities that can be exploited by an attacker. Unsupervised techniques, such as anomaly detection, can help us secure IoT devices. However, an anomaly detection model must be trained for a long time in order to capture all benign behaviors. This approach is weak in dealing with adversarial attacks since all observations are assumed to be benign while training an anomaly detection model.

We are researching a lightweight framework that utilizes the blockchain concept to perform distributed and collaborative anomaly detection for devices with limited resources. The framework uses blockchains to incrementally update a trusted anomaly detection model via self-attestation and consensus among IoT devices. We are evaluating the framework on our own distributed IoT simulation platform, which consists of 48 Raspberry Pis, to demonstrate the solution's ability to enhance the security of each device and the security of the network as a whole.

## Researchers

Tomer Golomb  
golombt@post.bgu.ac.il

Yisroel Mirsky  
yisroel@post.bgu.ac.il

Prof. Yuval Elovici  
elovici@inter.net.il

## Publications

T. Golomb, Y. Mirsky, and Y. Elovici, "CloTA: Collaborative Anomaly Detection via Blockchain," Workshop on Decentralized IoT Security and Standards [DISS], NDSS18, San Diego, 2018.

# Detering Attacks against Critical IT Infrastructure

## Researchers

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.

## 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 the 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.



# Securing MapReduce Computations Using Accumulating Automata

## Researchers

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

Shantanu Sharma  
sharmas@cs.bgu.ac.il

## 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,  $\Sigma$  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 illustrating the need for secure MapReduce using accumulating automata.



# DROPWAT: An Invisible Network Flow Watermark for Data Exfiltration Traceback

## Researchers

Dr. Alfonso Iacovazzi  
alfonso\_iacovazzi@sutd.edu.sg

Sanat Sarda  
sarda@sutd.edu.sg

Daniel Frassinelli  
frassinelli@sutd.edu.sg

Prof. Yuval Elovici  
elovici@inter.net.il

## Publications

A. Iacovazzi, S. Sarda, D. Frassinelli, and Y. Elovici, "DROPWAT: an Invisible Network Flow Watermark for Data Exfiltration Traceback," 2017. arXiv:1705.09460.

## Goals

Watermarking techniques have been proposed during the last 10 years as an approach to trace network flows for intrusion detection purposes. These techniques aim to impress a hidden signature on a traffic flow. A central property of network flow watermarking is invisibility, i.e., the ability to go unidentified by an unauthorized third party. Although widely sought after, the development of an invisible watermark is a challenging task that has not yet been accomplished.

## Description

We take a step forward in addressing the invisibility problem with DROPWAT, an active network flow watermarking technique developed for tracing Internet flows directed to the staging server that is the final destination in a data exfiltration attack, even in the presence of several intermediate stepping stones or an anonymous network. DROPWAT is a timing-based technique that indirectly modifies interpacket delays by exploiting network reaction to packet loss. We empirically demonstrate that the watermark embedded by means of DROPWAT is invisible to a third party observing the watermarked traffic. We also validate DROPWAT and analyze its performance in a controlled experimental framework involving the execution of a series of experiments on the Internet, using Web proxy servers as stepping stones executed on several instances in Amazon Web Services, as well as the TOR anonymous network, in place of the stepping stones. Our results show that the detection algorithm is able to identify an embedded watermark with over 95% accuracy while remaining invisible.



# Network Flow Watermarking: A Survey

## Description

Traffic analysis (TA) is a useful tool aimed at understanding network traffic behavior. Basic network administration often takes advantage of TA for purposes such as security, intrusion detection, traffic shaping and policing, diagnostic monitoring, provisioning, and resource management. Network flow watermarking is a type of TA in which packet features of selected flows are manipulated in order to add a specific pattern easily identifiable when the watermarked flows cross an observation point. While passive TA has been extensively studied, active TA, and more specifically network flow watermarking, has only recently attracted attention. Enforced robustness against traffic perturbations due to either natural network noise or attacks against passive TA have enhanced the appeal of this technique. The contribution of this project is a thorough review of the main watermarking algorithms implemented for traffic analysis purposes. We present an overview of the motivations and the objectives that have led to the use of network flow watermarking. We also describe the general architecture of a watermarking system. In addition, we impose clarity and order in this branch of TA by providing a taxonomy of the algorithms proposed in the literature over the years, and categorize and present them based on carrier, visibility, and robustness.

## Researchers

Dr. Alfonso Iacovazzi  
alfonso\_iacovazzi@sutd.edu.sg

Prof. Yuval Elovici  
elovici@inter.net.il

## Publications

A. Iacovazzi and Y. Elovici, "Network Flow Watermarking: A Survey," IEEE Communications Surveys & Tutorials, Vol. 19, Issue 1, 2017, pp. 512-530.



# INFLOW: Inverse Network Flow Watermarking for Detecting Hidden Servers

## Researcher

Dr. Alfonso Iacovazzi  
alfonso\_iacovazzi@sutd.edu.sg

sanat Sarda  
sarda@sutd.edu.sg;

Prof. Yuval Elovici  
elovici@inter.net.il

## Publications

A. Iacovazzi, S. Sarda, D. Frassinelli, and Y. Elovici, "INFLOW: Inverse Network Flow Watermarking for Detecting Hidden Servers," IEEE-INFOCOM 2018, Honolulu, 2018.

## Goals

Tor is a well-known and established communication system which allows its users to browse and communicate anonymously with fully guaranteed privacy, confidentiality, and content/service accessibility. When a content spreader needs to offer its content without being identified, they can use the hidden service system provided by the TOR network. However, this service has been increasingly abused, by distributing and hosting content, in most cases graphic, that are illegal or morally deplorable (e.g., child pornography). Law enforcement are continuously searching for means of identifying users and providers of such services. State-of-the-art techniques to breach the TOR anonymity are usually based on passive and active network traffic

analysis, controlling TOR edge communication and exploiting TOR inherent flow transfer mechanism. Nonetheless, detecting hidden servers and linking illegal contents with the spreaders is still a challenging task that has not been completely accomplished.

## Description

In this project, we describe INFLOW, a new technique to identify hidden servers based on inverse flow watermarking. INFLOW exploits the influence of congestion mechanisms on the traffic passing through the TOR network. INFLOW drops bursts of packets for short time intervals at the receiving side of a traffic flow coming from a hidden server and passing through the TOR network. Packet dropping affects the TOR flow control and causes time gaps in flows observed at the hidden server side. By controlling the communication edges and detecting the watermarked gaps, INFLOW is able to locate the hidden server. Our results, obtained by means of experiments performed on the real TOR network, show true positive rates in the range 90-98%.

## Researchers

Prof. Yossi Oren  
yos@bgu.ac.il

Yehonatan Tsionov  
Anatoly Shusterman  
Rom Ogen  
Adar Ovadya  
Liron Avraham  
Amir Cohen  
Benyamin Farshteindiker  
Omer Shwartz  
Hen Hayoon

## Publications

Y. Oren, "Side-channel Attacks Pose Growing Threat to Secrecy," IHS Jane's Intelligence Review Volume 29, Issue 9, September 2017.

O. Shwartz, et al., "Opening Pandora's Box: Effective Techniques for Reverse Engineering IoT Devices," 17th Smart Card Research and Advanced Application Conference [CARDIS], 2017.

O. Shwartz, et al., "Shattered Trust: When Replacement Smartphone Components Attack," 11th USENIX Workshop on Offensive Technologies [WOOT], 2017.

B. Farshteindiker, et al., "How to Phone Home with Someone Else's Phone: Information Exfiltration Using Intentional Sound Noise on Gyroscopic Sensors," 10th USENIX Workshop on Offensive Technologies [WOOT], 2016.

## Patent Applications

Y. Oren, A. Shabtai, O. Shvartz, A. Cohen, "Protecting a Device from Malicious Field Replaceable Units," US Patent Application.

Y. Oren, A. Grosz, N. Hasidim, and B. Farshteindiker, "Acoustic Security Code Transmission," US Patent Application.

# When Replacement Smartphone Components Attack

## Goals

The group at the Implementation Security Lab are researching side-channel attacks: cyber-attacks that allow the extraction of secret information from various devices by exploiting their precise physical behaviors (such as power consumption, electromagnetic emanations, heat or vibrations). Most recently they are looking at the threats posed by phone touchscreens and other hardware components, such as orientation sensors and NFC readers, where third-party driver source code to support these components is integrated into the vendor's source code with very few integrity checks.

## Description

The research conducted in the lab is grounded in knowledge attained as part of the EU-funded ECRYPT project and uses precise measurement equipment and techniques to assess the impact of side-channel attacks by measuring the leakage of target devices under tests. This allows the researchers to obtain an upper bound on the potential performance of attacks carried out using less sensitive measurement devices such as compromised phones or malicious aftermarket peripherals.

In recent testing, they were able to construct two standalone attacks, based on malicious touchscreen hardware, that function as building blocks toward a full attack: a series of touch injection attacks that allow the touchscreen to impersonate the user and exfiltrate data, and a buffer overflow attack that lets the attacker execute privileged operations. Their results make the case for a hardware-based physical countermeasure.

In addition, Dr. Oren plans to use this lab to find creative and unexpected uses for the sensors found on modern mobile phones, such as the gyroscope, touch screen, and magnetic compass.



# A Lightweight Vulnerability Mitigation Framework for IoT Devices

## Researchers

Noy Hadar  
noyhada@post.bgu.ac.il

Shachar Siboni  
shachar.siboni@gmail.com

Prof. Yuval Elovici  
elovici@inter.net.il

## Publications

N. Hadar, S. Siboni, and Y. Elovici, "A Lightweight Vulnerability Mitigation Framework for IoT Devices," Proceedings of the Workshop on Internet of Things Security and Privacy [IoTS&P], 2017, pp. 71-75.

## Description

Many of today's Internet of Things (IoT) devices are vulnerable due to the large amount of overhead incurred when their operating systems are patched against emerging vulnerabilities. In addition, legacy IoT devices are no longer supported by their manufacturers, leaving customers with unpatched devices that can be easily exploited by attackers. Thus, there is an urgent need for a solution that provides a lightweight and low-cost mechanism for preventing exploitation of vulnerable IoT devices. We propose an innovative cloud-based framework for protecting IoT devices. The proposed framework consists of a cloud service and a designated IoT security appliance. The security appliance controls the network traffic flowing to and from the vulnerable device and verifies that it does not violate a set of rules, represented by a vulnerability mitigation policy, that have been derived and synthesized by the cloud service from public corpora of Common Vulnerabilities and Exposures (CVE). We demonstrate how the proposed solution can be applied as a cost-effective solution capable of preventing exploitation of vulnerable IP cameras as part of a prominent botnet attack called Mirai.

### Researchers

Dr. Asaf Shabtai  
shabtaia@bgu.ac.il

Prof. Yuval Elovic  
elovici@inter.net.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.

# 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.





# Handwritten Signature Verification Using Hand-Worn Devices

## Researchers

Ben Nassi  
nassib@post.bgu.ac.il

Alona Levy  
alonale1@mail.tau.ac.il

Prof. Yuval Elovici  
elovici@inter.net.il

Dr. Erez Shmueli  
shmueli@tau.ac.il

## Publications

B. Nassi, A. Levy, Y. Elovici,  
and E. Shmueli, "Handwritten  
Signature Verification Using  
Hand-Worn Devices," 2016.  
arXiv:1612.06305v1.

## Description

Online signature verification technologies, such as those available in banks and post offices, rely on dedicated digital devices, such as tablets or smart pens, to capture, analyze and verify signatures. We suggest a novel method for online signature verification that relies on increasingly available hand-worn devices, such as smartwatches or fitness trackers, instead of dedicated ad-hoc devices.

Our method uses a set of known genuine and forged signatures, recorded using the motion sensors of a hand-worn device, to train a machine learning classifier. Then, given the recording of an unknown signature and a claimed identity, the classifier can determine whether the signature is genuine or forged. In order to validate our method, it was applied on 1980 recordings of genuine and forged signatures that we collected from 66 subjects in our institution. Using our method, we were able to successfully distinguish between genuine and forged signatures with a high degree of accuracy (0.98 AUC and 0.05 EER).



# Independent Vehicle Authentication Using Non-fixed Attributes

## Researchers

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

Nisha Panwar  
panwar@cs.bgu.ac.il

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

## Results

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.

## 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's 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.

## Researchers

Dr. Nir Nissim  
nirni.n@gmail.com

Tom Mahler  
tommahler@gmail.com

Dr. Erez Shalom  
erezsh@post.bgu.ac.il

Israel Goldenberg  
israel@clalit.org.il

Guy Hasman  
GuyHa3@clalit.org.il

Dr. Arnon Makori, MD  
ArnonMa@clalit.org.il

Itzik Kochav  
kochav@clalit.org.il

Prof. Yuval Elovici  
elovici@inter.net.il

Prof. Yuval Shahr  
yshahr@bgu.ac.il

## Publications

N. Nissim, T. Mahler, E. Shalom, I. Goldenberg, G. Hasman, A. Makori, I. Kochav, Y. Elovici, and Y. Shahr, "Know Your Enemy: Characteristics of Cyber-Attacks on Medical Imaging Devices," RSNA Conference, Chicago, April 2017.

N. Nissim, E. Shalom, Y. Shahr, and Y. Elovici, "Cyber-Med: Risk Assessment and Practical Detection Methodology of Cyber-Attacks Aimed at Medical Device Eco-Systems," 18th International Conference on Big Data in Biomedicine [ICBDB], Buenos Aires, 2016.

# Know Your Enemy: Characteristics of Cyber Attacks on Medical Imaging Devices

## Description

Medical devices play increasingly important roles in health services eco-systems, including: (1) Patient Diagnostics and Monitoring, including digital devices that measure heart rate, blood glucose, blood pressure, radiology images, etc. Such devices monitor or deliver important pieces of information that are used by doctors to make medical decisions regarding the patient's medical care; alternatively, this information is used by the patient's supportive medical devices to overcome or compensate for failures in his/her body. (2) Medical Treatment and Surgery, such as radiotherapy for cancer patients, robots that conduct complicated surgeries, and laparoscopic instruments (e.g., the Da Vinci robot). (3) Patient Life Support Devices and Stabilizers including devices which can be implanted (such as pacemakers) or external devices (such as defibrillators, insulin pumps, etc.). Devices in the medical device eco-system are connected to the network, sending vital information (patients' measurements, diagnoses, imaging results, and surgical and treatment summaries) to the internal medical information systems of medical centers, such as Picture Archiving and Communication Systems (PACS) that manage this data. In addition, medical devices today also connected to the cloud, interacting with patient information in real time. Wireless components are often embedded within medical devices, enabling doctors and technicians to control and configure them remotely.

All these functionalities, roles, and uses of medical devices make them attractive targets of cyber-attacks launched for many malicious goals. This trend is likely to significantly increase over the next several years, with increased awareness regarding their vulnerabilities, the enhancement of potential attackers' skills, and expanded use of such devices.



# Context-based Data Leakage Detection

## Researchers

Prof. Yuval Elovici  
elovici@inter.net.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

## 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.



# Cyber-Med: Risk Assessment and Practical Detection Methodology of Cyber Attacks Aimed at Medical Device Ecosystems

## Researchers

Dr. Nir Nissim  
nirni.n@gmail.com

Erez Shalom  
erezsh@post.bgu.ac.il

Prof. Yuval Shahaar  
yshahaar@bgu.ac.il

Prof. Yuval Elovici  
elovici@inter.net.il

## Publications

N. Nissim, T. Mahler, E. Shalom, I. Goldenberg, G. Hasman, A. Makori, I. Kochav, Y. Elovici, and Y. Shahaar, "Know Your Enemy: Characteristics of Cyber-Attacks on Medical Imaging Devices," RSNA Conference, Chicago, 2017.

N. Nissim, E. Shalom, Y. Shahaar, and Y. Elovici, "Cyber-Med: Risk Assessment and Practical Detection Methodology of Cyber-Attacks Aimed at Medical Device Eco-Systems," 18th International Conference on Big Data in Biomedicine [ICBDB], Buenos Aires, 2016.

## Goals

In an initial survey, we found more than 15 types of vulnerabilities and possible attacks aimed at medical devices and their eco-system. Many of these attacks target individual patients who use devices such as pacemakers and insulin pumps. In addition, such attacks are also aimed at additional medical devices that are widely used by medical centers, such as MRIs, CTs, and dialysis engines; at the information systems that store patient information, including diagnoses (clinical images, test results, etc.), and are used as the basis for decisions related to patient care; at the information systems that store patient information, including diagnoses, and are used as the basis of decisions relating to patient care; at protocols such as DICOM; at standards such as HL7; and at medical information systems such as PACS.

Current detection tools, techniques, and solutions generally fail to detect both the known and unknown attacks launched against medical devices. Very little research has been conducted to protect these devices from cyber-attacks, since most of the development and engineering efforts are focused on core medical functionality, contribution to patient care, and associated business aspects.

We propose to develop and implement Cyber-Med, a unique collaborative project of Ben-Gurion University of the Negev and Clalit Health Services' Health Maintenance Organization.

## Description

Cyber-Med focuses on a thorough risk analysis of the vulnerabilities associated with medical devices and the development of a comprehensive detection framework that relies on a critical attack repository that we aim to create. The Cyber-Med detection framework will consist of two independent, but complementary detection approaches: one for known attacks, and the other for unknown attacks. These modules incorporate novel ideas and algorithms inspired by our team's domains of expertise, including cyber security, biomedical informatics, and advanced machine learning, and temporal data mining techniques. Establishment and maintenance of Cyber-Med's attack repository will strengthen Cyber-Med's detection framework. The attack repository's infrastructure will enable researchers to record, document, create, and simulate existing and new attacks on MDs, which, in turn, will maintain the detection framework's capabilities by incorporating up-to-date knowledge regarding new attacks.



# Self-Stabilizing Cloud Infrastructure

## Researchers

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

Dr. Alexander Binun  
binun@cs.bgu.ac.il

Dr. Reuven Yagel  
yagel@cs.bgu.ac.il

Tomer Godinger  
tomergod@post.bgu.ac.il

Mark Bloch  
markbl@post.bgu.ac.il

Boaz Menuhin  
boaz.menuhin@gmail.com

Martin Kahil  
kahil@post.bgu.ac.il

## Goals

The main goal is to obtain a robust self-stabilizing cloud. Such a cloud will need far less human intervention to function and will be capable of fast recovery from various attacks.

The intermediate goal is to build a self-stabilizing local hypervisor that ensures smooth and correct execution of each Virtual Machine (VM) and protects it from negative effects posed by malware attacks and possible Byzantine behavior of VMs in a system.

Eventually we aim to extend the self-stabilizing local hypervisor to the distributed cloud. We intend to achieve this goal using the open-source distributed cloud provider OpenStack.

## Description

Our self-stabilizing hypervisor demonstrates robustness in the presence of transient faults in VMs and Byzantine VMs. The cloud is becoming more and more popular, thus the need for resource utilization. All cloud providers exploit virtualization to achieve optimal 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. Rigid security policies may decrease system performance and/or restrict collaborations, thus potentially affecting service level agreements (SLAs). An automatically recovering system of virtual machines helps provide security, while still meeting SLAs, making a great contribution to the field.

We have developed a self-stabilizing architecture, augmenting the widely known KVM hypervisor with self-stabilization facilities. A system comprising several VMs is able to recover after transient failures and attacks (e.g. denial of service, worms, corruption of sensitive memory areas).

We are currently extending the prototype into the distributed world. We are deploying and running attack scenarios on OpenStack, simulating the comprehensive attack model and the approach to recover a distributed cloud. We note that, during the first research phase, the defenses against certain threats were hardcoded into our module. During the following phase, we support generic user-defined defense specifications.

This 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.

# Activity-based Verification

## Continuous User Verification after Successful Login

### Researchers

Yisrael Mirsky  
ymirsky1@gmail.com

Prof. Yuval Elovici  
elovici@inter.net.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]*, 411-41.

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 e-mail 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.



# Oops!.. I Think I Scanned a Malware

## Researchers

Ben Nassi  
nassidt@gmail.com

Prof. Adi Shamir  
adi.shamir@weizmann.ac.il

Prof. Yuval Elovici  
elovici@inter.net.il

## Publications

B. Nassi, A. Shamir, Y. Elovici,  
“Oops!.. I think I scanned a  
malware,” 2017. arXiv:1703.07751.

## Description

The researchers present a proof-of-concept illustrating the feasibility of creating a covert channel between a C&C server and a malware installed in an organization by exploiting an organization’s scanner and using it as a means of interaction. We take advantage of the light sensitivity of a flatbed scanner, using a light source to infiltrate data to an organization. We present an implementation of the method for different purposes (even to trigger a ransomware attack) in various experimental setups using: (1) a laser connected to a stand (2) a laser carried by a drone, and (3) a hijacked smart bulb within the organization targeted by a passing car. In our experiments we were able to infiltrate data using different types of light sources (including infrared light), from a distance of up to 900 meters away from the scanner. We discuss potential counter measures to prevent the attack.





# Socialbots Studies

## Researchers

Aviad Elyashar  
aviade@post.bgu.ac.il

Michael Fire  
mickyfi@post.bgu.ac.il

Dima Kagan  
kagandi@post.bgu.ac.il

Prof. Yuval Elovici  
elovici@inter.net.il

## Publications

Aviad Elyashar, Michael Fire, Dima Kagan, and Yuval Elovici, "Organizational Intrusion: Organization Mining Using Socialbots," 2012 International Conference on Social Informatics [SocialInformatics].

Aviad Elyashar, Michael Fire, Dima Kagan, and Yuval Elovici, "Homing Socialbots: Intrusion on a Specific Organization's Employee Using Socialbots," International Workshop on Social Network Analysis in Applications [SNAA], co-located with ASONAM 2013, Niagara Falls, Canada, August 2013.

Aviad Elyashar, Michael Fire, Dima Kagan, and Yuval Elovici, "Guided Socialbots: Infiltrating User's Friends List," AI Communications, 2014.

## Goals

In recent years, adversaries have taken advantage of online social networks in order to collect private information regarding users, such as e-mail addresses, phone numbers, and other personal data that have monetary value. Such information can then be used for online profiling and large-scale e-mail spamming and phishing campaigns. We have two major goals: first, we seek to demonstrate how easy it is to extract private information about a specific organization's employees using socialbots. Second, we use socialbots to infiltrate employees' private social networks. By means of these infiltrations, we are able to study targeted organizations and their employees.

## Description

In the first study, we introduced a method for mining an organization's information through social networks and socialbots. We created socialbots and used them to send friend requests to Facebook users who worked at a targeted organization. By accepting friend requests through socialbots, users exposed information about themselves and about their workplace. We tested the proposed method on two real organizations and successfully infiltrated both of them. Compared to our previous studies, our method was able to discover up to 13.55% more employees and up to 18.29% more informal organizational links.

In the second study, we introduced a method for attacking specific users in targeted organizations by using organizational social network topologies and socialbots. To target users, we randomly chose ten Facebook users from every targeted organization. Our socialbots sent friend requests to all the specific users' mutual friends who worked or work in the same targeted organization. The rationale was to gain as many mutual friends as possible and thus increase the probability that our friend requests would be accepted by the targeted users. We tested the proposed method on targeted users from two different organizations. Our method achieved success rates of 50% and 70%, respectively, among the ten targeted users.

In the last study, we enhanced our previous study and evaluated our suggested method for infiltrating key employees of targeted organizations on two well-known OSNs – Facebook and Xing. The results obtained demonstrate how adversaries can infiltrate social networks to gain access to valuable private information regarding employees and their organizations. Moreover, the results indicate that users who wish to protect themselves should not disclose information on online social networks and should be cautious of accepting friend requests from unknown persons.



# Taxonomy of Mobile Users' Security Awareness

## Researchers

Ron Bitton  
bittonron@gmail.com

Andrey Finkelstein  
andreyfi@post.bgu.ac.il

Lior Sidi  
liorsid@post.bgu.ac.il

Dr. Rami Puzis  
puzis@bgu.ac.il

Prof. Lior Rokach  
liorrk@bgu.ac.il

Dr. Asaf Shabtai  
shabtaia@bgu.ac.il

## Goals

The popularity of smartphones, coupled with the amount of valuable and private information they hold, make them attractive to attackers interested in exploiting the devices to harvest sensitive information. Improving the security awareness of users is an effective method for mitigating social engineering attacks. However, while the security awareness of PC users is relatively high, studies have shown that for the mobile platform, the security awareness level is significantly lower. The skills required from a mobile user to interact safely with his/her smartphone are different from those that are required for PC use. Therefore, the awareness of mobile users to security risks is an important aspect of information security. An essential and challenging requirement of assessing security awareness is the definition of measurable criteria for a security aware user.

## Description

The researchers have developed a hierarchical taxonomy for security awareness, specifically designed for mobile device users. The taxonomy defines a set of measurable criteria that are categorized according to different technological focus areas (e.g., applications and browsing) and within the context of psychological dimensions (e.g., knowledge, attitude, and behavior). They demonstrate the applicability of the proposed taxonomy by introducing an expert-based procedure for deriving mobile security awareness models for different attack classes (each class is an aggregation of social engineering attacks that exploit a similar set of human vulnerabilities). Each model reflects the contribution (weight) of each criteria to the mitigation of the corresponding attack class. Application of the proposed procedure, based on the input of 17 security experts, to derive mobile security awareness models of four different attack classes, confirms that the skills required from a smartphone user to mitigate an attack are different for different attack classes.

# Game of Drones: Detecting Streamed POI from Encrypted FPV Channel

## Researchers

Ben Nassi  
nassidt@gmail.com

Raz Ben-Netanel  
razx@post.bgu.ac.il

Prof. Adi Shamir  
adi.shamir@weizmann.ac.il

Prof. Yuval Elovici  
elovici@inter.net.il

## Publication



B. Nassi, R. Ben-Netanel, A. Shamir, and Yuval Elovici, "Game of Drones - Detecting Streamed POI from Encrypted FPV Channel, 2018. arXiv:1801.03074.

## Goals

Drones have created a new threat to people's privacy. We are now in an era in which anyone with a drone equipped with a video camera can use it to invade a subject's privacy by streaming the subject in his/her private space over an encrypted first person view (FPV) channel. Although many methods have been suggested to detect nearby drones, they all suffer from the same shortcoming: they cannot identify exactly what is being captured, and therefore they fail to distinguish between the legitimate use of a drone (for example, to use a drone to film a selfie from the air) and illegitimate use that invades someone's privacy (when the same operator uses the drone to stream the view into the window of his neighbor's apartment), a distinction that in some cases depends on the orientation of the drone's video camera rather than on the drone's location.

## Description

We challenge the commonly held belief that the use of encryption to secure an FPV channel prevents an interceptor from extracting the POI that is being streamed. We show methods that leverage physical stimuli to detect whether the drone's camera is directed towards a target in real time. We investigate the influence of changing pixels on the FPV channel (in a lab setup). Based on our observations we demonstrate how an interceptor can perform a side-channel attack to detect whether a target is being streamed by analyzing the encrypted FPV channel that is transmitted from a real drone (DJI Mavic) in two use cases: when the target is a private house and when the target is a subject.



# VisiSploit: An Optical Covert-channel to Leak Data through an Air-gap

## Researchers

Dr. Mordechai Guri  
moti.guri@gmail.com

Ofar Hasson  
hassonofar@gmail.com

Gabi Kedma  
gabikedma@hotmail.com

Prof. Yuval Elovici  
elovici@inter.net.il

## Publications

M. Guri, O. Hasson, G. Kedma, and Y. Elovici, "VisiSploit: An Optical Covert-Channel to Leak Data through an Air-Gap," 2016. arXiv:1607.03946.

## Goals

In recent years, various out-of-band covert channels have been proposed that demonstrate the feasibility of leaking data out of computers without the need for network connectivity. The methods proposed have been based on different type of electromagnetic, acoustic, and thermal emissions. However, optical channels have largely been considered less covert: Because they are visible to the human eye and hence can be detected, they have received less attention from researchers.

We introduce VisiSploit, a new type of optical covert channel which, unlike other optical methods, is also stealthy.

## Description

Our method exploits the limitations of human visual perception in order to unobtrusively leak data through a standard computer LCD display. Our experiments show that very low contrast or fast flickering images (which are invisible to human subjects) can be recovered from photos taken by a camera. Consequentially, we show that malicious code on a compromised computer can obtain sensitive data (e.g., images, encryption keys, passwords) and project it onto a computer LCD screen, invisible and unbeknownst to users, allowing an attacker to reconstruct the data using a photo taken by a nearby (possibly hidden) camera. In order to demonstrate the feasibility of this type of attack and evaluate the channel's stealth, we conducted a battery of tests with 40 human subjects. We also examined the channel's boundaries under various parameters, with different types of encoded objects, at several distances, and using several kinds of cameras. Our results show that binary data can be leaked via our covert channel. Further research and discussion may widen the scope of this field beyond its current boundaries, yielding novel attack paradigms that exploit the subtle mechanisms of human visual perception.



# LED-it-GO: Leaking (a lot of) Data from Air-gapped Computers via the (small) Hard Drive LED

## Description

We present a method which allows attackers to covertly leak data from isolated, air-gapped computers. Our method utilizes the hard disk drive (HDD) activity LED which exists in most of today's desktop PCs, laptops and servers. We show that a malware can indirectly control the HDD LED, turning it on and off rapidly (up to 5800 blinks per second), a rate that exceeds the visual perception capabilities of humans. Sensitive information can be encoded and leaked over the LED signals, which can then be received remotely by different kinds of cameras and light sensors. Compared to other LED methods, our method is unique, because it is also covert: The HDD activity LED routinely flickers frequently, and therefore the user may not be suspicious to changes in its activity.

We discuss attack scenarios and present the necessary technical background regarding the HDD LED and its hardware control. We also present various data modulation methods and describe the implementation of a user-level malware that doesn't require a kernel component. We examined the physical characteristics of different colored HDD LEDs (red, blue, and white) and tested different types of receivers: remote cameras, extreme cameras, security cameras, smartphone cameras, drone cameras, and optical sensors. Our experiment shows that sensitive data can be successfully leaked from air-gapped computers via the HDD LED at a maximum bit rate of 4000 bits per second, depending on the type of receiver and its distance from the transmitter. Notably, this speed is 10 times faster than the existing optical covert channels for air-gapped computers. These rates allow fast exfiltration of encryption keys, keystroke logging, and text and binary files. Finally, we also discuss hardware and software countermeasures for such a threat.

## Researchers

Dr. Mordechai Guri  
moti.guri@gmail.com

Boris Zadov  
borisza@gmail.com

Eran Atias  
eran\_ats@walla.co.il

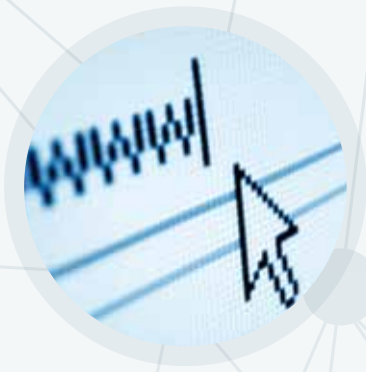
Prof. Yuval Elovici  
elovici@inter.net.il

## Publications

M. Guri, B. Zadov, E. Atias, and Y. Elovici, "LED-It-GO: Leaking [a lot] of Data from Air-Gapped Computers via the [small] Hard Drive LED," 2017. arXiv:1702.06715.

## Demo Video

<https://www.youtube.com/watch?v=4vlu8ld68fc>



# Identifying URLs for Blacklist

## Researchers

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

Dr. Rami Puzis  
puzis@bgu.ac.il

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

## 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, 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.



# Data Leakage Detection in Social Networks

## Researchers

Prof. Yuval Elovici  
elovici@inter.net.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.



# Detecting Anti-Forensic APTs

## Researchers

Prof. Yuval Elovici  
elovici@inter.net.il

Mordechai Guri  
gurim@post.bgu.ac.il

Gabi Kedma  
gabik@post.bgu.ac.il

## Publications

“Non-Invasive Detection of Anti-Forensic Malware,”  
Malware 2013 Conference.

## 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 research we propose a new method to detect and classify antiforensic 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.





# SecretSkyDB

## Researchers

Prof. Shlomi Dolev  
shlomidolev@gmail.com

Dr. Ximing Li  
liximing.cn@gmail.com

Dr. Yin Li  
yunfeiyangli@gmail.com

## Results

A multi-cloud database product is being developed as a startup company in collaboration with JVP Cyber Labs.

Patent assigned to SecretSkyDB.

## Goals

Next generation private database.

## Description

SecretSkyDB (Secret Sky) is based on the random distribution of each piece of information on each of the participating storages, while still defining exactly the information when accessing the participating storages. Thus, one may store personal photos, letters, and passwords on Google, Amazon, Microsoft, and IBM clouds without revealing any useful information to any of them. Prof. Shlomi Dolev and post-docs on his team have designed innovative schemes to search, in parallel, the distributed storages (each of which was holding useless information) and return the required data item. In fact, they were able to execute programs on distributed data without even revealing the program.

Key value database was implemented as part of the Kamin grant that started prior to the activity on Secret Double Octopus, and together with patents on the technology, were used to establish SecretSkyDB.

# Personal Information Leakage through Online Social Networking: Leakage Prevention and Leakers Detection

## Researchers

Yasmin Bokobza  
yasminbo@post.bgu.ac.il

Prof. Bracha Shapira  
bshapira@bgu.ac.il

Dr. Rami Puzis  
puzis@bgu.ac.il

Prof. Lior Rokach  
liorrk@bgu.ac.il

## Goals

The explosion of online social networking in recent years has damaged organizations due to information leakage by their employees. Employees' social networking activity provides an opportunity for adversaries to extract information from Online Social Networks (OSNs) that may not appear on the official organizational website. This new reality has forced organizations to recognize the need to pay closer attention to the use of OSNs by their employees. For large organizations with thousands of employees, analysis of the content to which all employees are exposed or distribute is unfeasible. Detecting private information leakage and identifying the employees at the source of the leaks are very complex tasks.

## Description

In this research, we detect unintentional private information leakage by employees on social networking sites as soon as possible by intelligently selecting organization member profiles and monitoring their activity. We propose and evaluate efficient SN crawling strategies that are based on topology and central features of the users, such as the number of followers and page rank scoring.

Once we detect private information leakage, we would like to identify the employee at the source of the leak. In order to detect a leaker, the friends of a monitored profile must be inspected. This inspection includes analyzing the content to which these friends were exposed or distributed. We propose and evaluate strategies for identifying the employees who leak private information, with emphasis on high precision and minimal time and effort.

## Results

We used three datasets: Flickr, Digg and Ning. In our evaluation we identified communities within the social networks and referred to each community as an organization. To identify the communities, we used the label propagation algorithm, since it runs in nearly-linear time, allowing for the analysis of large OSN data sets.

Our results show that by monitoring the activity of the users with the highest page rank scoring we can detect more leaks with less effort, by monitoring fewer users. Moreover, by inspecting the friends of a monitored profile with the highest number of followers, we identify more leakers in minimal time and effort.



# Generic Black-Box End-to-End Attack against RNNs and Other API Call-based Malware

## Researchers

Ishai Rosenberg  
ishairos@post.bgu.ac.il

Dr. Asaf Shabtai  
shabtaia@bgu.ac.il

Prof. Lior Rokach  
liorrk@bgu.ac.il

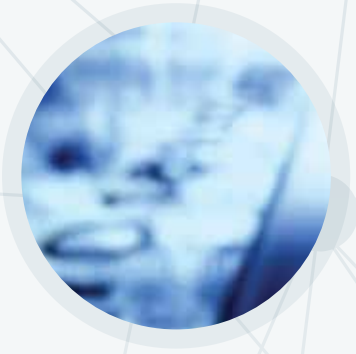
Prof. Yuval Elovici  
elovici@inter.net.il

## Publications

I. Rosenberg, A. Shabtai, L. Rokach, and Y. Elovici, "Generic Black-Box End-to-End Attack Against State of the Art API Call Based Malware Classifiers," 2017. arXiv:1707.05970.

## Description

We present a black-box attack against API call-based machine learning malware classifiers, focusing on generating adversarial API call sequences that would be misclassified by the classifier without affecting the malware functionality. We show that this attack is effective against many classifiers due to the transferability principle between RNN variants, feed forward DNNs, and traditional machine learning classifiers such as SVM. We further extend our attack against hybrid classifiers based on a combination of static and dynamic features, focusing on printable strings and API calls. Finally, we implement GADGET, a software framework to convert any malware binary to a binary undetected by malware classifiers, using the proposed attack, without access to the malware source code. We conclude by discussing possible defense mechanisms against the attack.



# Context Aware Data Leakage Prevention for Mobile Devices

## Researchers

Prof. Lior Rokach  
liorrk@bgu.ac.il

Dr. Asaf Shabtai  
shabtaia@bgu.ac.il

Prof. Yuval Elovici  
elovici@inter.net.il

Prof. Bracha Shapira  
bshapira@bgu.ac.il

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

## 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's long-term storage, or retrieved from the cloud using credentials that are stored in the device. 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.





# USBee: Air-gap Covert-channel via Electromagnetic Emission from USB

## Researchers

Dr. Mordechai Guri  
moti.guri@gmail.com

Matan Monitz  
mmonitz@gmail.com

Prof. Yuval Elovici  
elovici@inter.net.il

## Publications

M. Guri, M. Monitz, and Y. Elovici,  
“USBee: Air-Gap Covert-Channel  
via Electromagnetic Emission from  
USB,” 2016. arXiv:1608.08397.

## Demo Video

[https://www.youtube.com/  
watch?v=E28V1t-k8Hk](https://www.youtube.com/watch?v=E28V1t-k8Hk)

## Goals

In recent years researchers have demonstrated how attackers could use USB connectors implanted with RF transmitters to exfiltrate data from secure, and even air-gapped, computers (e.g., COTTONMOUTH in the leaked NSA ANT catalog). Such methods require a hardware modification of the USB plug or device, in which a dedicated RF transmitter is embedded. We present ‘USBee’, a software that can utilize an unmodified USB device connected to a computer as a RF transmitter.

## Description

We demonstrate how a software can intentionally generate controlled electromagnetic emissions from the data bus of a USB connector. We also show that the emitted RF signals can be controlled and modulated with arbitrary binary data. We implemented a prototype of USBee, and discuss here its design and implementation details, including signal generation and modulation. We also evaluated the transmitter by building a receiver and demodulator using GNU Radio. Our evaluation shows that USBee can be used for transmitting binary data to a nearby receiver at a bandwidth of 20 to 80 BPS (bytes per second).

# DiskFiltration: Data Exfiltration from Speakerless Air-gapped Computers via Covert Hard Drive Noise

## Researchers

Dr. Mordechai Guri  
moti.guri@gmail.com

Dr. Yosef Solewicz  
yosef.solewicz@gmail.com

Andrey Daidakulov  
daidakul@post.bgu.ac.il

Prof. Yuval Elovici  
elovici@inter.net.il

## Publications

M, Guri, Y. Solewicz, A. Daidakulov, and Y. Elovici, "DiskFiltration: Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard Drive Noise," 2016. arXiv:1608.03431.

## Demo Video

<https://www.youtube.com/watch?v=H71QXmSLIP8>

## Goals

Air-gapped computers are disconnected from the Internet physically and logically. This measure is taken in order to prevent the leakage of sensitive data from secured networks. It has been shown that malware can exfiltrate data from air-gapped computers by transmitting ultrasonic signals via the computer's speakers. However, such acoustic communication relies on the availability of speakers on a computer.

We present 'DiskFiltration,' a covert channel which facilitates the leakage of data from an air-gapped compute via acoustic signals emitted from its hard disk drive (HDD).

## Description

Our 'DiskFiltration' method is unique in that, unlike other acoustic covert channels, it doesn't require the presence of speakers or audio hardware in the air-gapped computer. A malware installed on a compromised machine can generate acoustic emissions at specific audio frequencies by controlling the movements of the HDD's actuator arm. Digital information can be modulated over the acoustic signals and then be picked up by a nearby receiver (e.g., smartphone, smartwatch, laptop, etc.). We examine the HDD anatomy and analyze its acoustical characteristics. We also present signal generation and detection, and data modulation and demodulation algorithms. Based on our proposed method, we developed a transmitter on a personal computer and a receiver on a smartphone. We also evaluated our covert channel on various types of internal and external HDDs in different computer chassis and at various distances. With 'DiskFiltration' we were able to covertly transmit data (e.g., passwords, encryption keys, and keylogging data) between air-gapped computers to a smartphone at an effective bit rate of 180 bits/minute (10,800 bits/hour) and a distance of up to two meters (six feet).



# Social Network Digestion

## Researchers

Prof. Yuval Elovici  
elovici@inter.net.il

Dr. Rami Puzis  
puzis@bgu.ac.il

Michael Fire  
mickyfi@post.bgu.ac.il

## 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," SNA 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 AAI-13, Bellevue, Washington, USA, and in BISFAI 2013

Zahy Bnaya, Rami Puzis, Roni Stern, and Ariel Felner, "Volatile Multi-Armed Bandits for Guaranteed Targeted Social Crawling", In AAI-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



# Unknown Malware Detection Using Network Flow Pattern Classification

## Researchers

Dimitri Bekerman  
bekerDMI@post.bgu.ac.il

Prof. Bracha Shapira  
bshapira@bgu.ac.il

Prof. Lior Rokach  
liorrk@bgu.ac.il

## Goals

Common computer malwares are smart, persistent and have the ability to hide themselves from the most modern anti-malware software, yet when such a malware tries to communicate with the rest of the world it most likely uses common known protocols to pass through the firewalls and network intrusion detection systems. Unfortunately, all those systems are based on static rules created manually by cyber security engineers based on previous intrusions.

Our aim is to develop a method that is based on machine learning techniques for detecting previously unknown malicious activities and in particular malware's communication with command and control servers, thus enabling the system to dynamically and independently infer the detection rule.

## Description

During this research we developed cross layer attributes for network traffic aggregation to induce a reliable classifier, and classify benign and malware network traffic. Those attributes are based on DNS address resolution patterns, statistical analysis of HTTP and HTTPs transactions and network-flow anomalies of incoming and outgoing traffic. The classification model has been specifically designed to deal with NATed and encrypted traffic and also to handle high throughput networks.

## Results

We evaluated our classification model on malicious captures from various sandboxes as well as from a real high bandwidth network. We managed to detect previously unknown malwares with high accuracy, with tolerable false alarm rates.



# Fansmitter: Acoustic Data Exfiltration from (Speakerless) Air-gapped Computers

## Researchers

Dr. Mordechai Guri  
moti.guri@gmail.com

Dr. Yosef Solewicz  
yosef.solewicz@gmail.com

Andrey Daidakulov  
daidakul@post.bgu.ac.il

Prof. Yuval Elovici  
elovici@inter.net.il

## Publications

M. Guri, Y. Solewicz, A. Daidakulov, and Y. Elovici, "Fansmitter: Acoustic Data Exfiltration from [Speakerless] Air-Gapped Computers," 2016. arXiv:1606.05915.

## Demo video

[https://www.youtube.com/watch?v=v2\\_sZlfZkDQ](https://www.youtube.com/watch?v=v2_sZlfZkDQ)

## Goals

Because computers may contain or interact with sensitive information, they are often air-gapped and thus kept isolated and disconnected from the Internet. In recent years the ability of malware to communicate over an air-gap by transmitting sonic and ultrasonic signals from a computer speaker to a nearby receiver has been demonstrated. In order to eliminate such acoustic channels, current best practice recommends the elimination of speakers (internal or external) in secure computers, thereby creating a so-called 'audio-gap.' In this paper, we present 'Fansmitter,' a malware that can acoustically exfiltrate data from air-gapped computers, even when audio hardware and speakers are not present.

## Description

The 'Fansmitter' method utilizes the noise emitted from the CPU and chassis fans, which are present in virtually every computer. We show that a software can regulate the internal fans' speed in order to control the acoustic waveform emitted from the computer. Binary data can be modulated and transmitted over these audio signals to a remote microphone (e.g., on a nearby mobile phone). We present Fansmitter's design considerations, including acoustic signature analysis, data modulation, and data transmission. We also evaluate the acoustic channel, present our results, and discuss countermeasures.

Using our method we successfully transmitted data from an air-gapped computer without audio hardware to a smartphone receiver in the same room. We demonstrated the effective transmission of encryption keys and passwords from a distance of zero to eight meters, with bit rate of up to 900 bits/hour. We also demonstrated that our method can be used to leak data from different types of IT equipment, embedded systems, and IoT devices that have no audio hardware, but contain fans of various types and sizes.



# GSMem: Data Exfiltration from Air-gapped Computers over GSM Frequencies

## Researchers

Dr. Mordechai Guri  
moti.guri@gmail.com

Assaf Kachlon  
assafka@post.bgu.ac.il

Ofer Hasson  
hassonofer@gmail.com

Gabi Kedma  
gabikedma@hotmail.com

Yisroel Mirsky  
yisroel@post.bgu.ac.il

Prof. Yuval Elovici  
elovici@inter.net.il

## Publications

M. Guri, A. Kachlon, O. Hasson, G. Kedma, Y. Mirsky, and Y. Elovici, "GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies," 24th USENIX Security Symposium, Washington DC, 2016.

## Demo video

<https://www.youtube.com/watch?v=RChj7Mg3rC4>

## Goals

Air-gapped networks are isolated, separated both logically and physically from public networks. Although the feasibility of invading such systems has been demonstrated in recent years, exfiltration of data from air-gapped networks is still a challenging task. We present GSMem, a malware that can exfiltrate data through an air-gap over cellular frequencies.

## Description

We demonstrate how rogue software on an infected target computer modulates and transmits electromagnetic signals at cellular frequencies by invoking specific memory-related instructions and utilizing the multichannel memory architecture to amplify the transmission. Furthermore, we show that the transmitted signals can be received and demodulated by a rootkit placed in the baseband firmware of a nearby cellular phone. We present crucial design issues, such as signal generation and reception, data modulation, and transmission detection. We implement a prototype of GSMem consisting of a transmitter and a receiver and evaluate its performance and limitations. Our current results demonstrate its efficacy and feasibility, achieving an effective transmission distance of 1-5.5 meters with a standard mobile phone. When using a dedicated, yet affordable hardware receiver, the effective distance reached over 30 meters.

# BitWhisper: Covert Signaling Channel Between Air-gapped Computers Using Thermal Manipulations

## Researchers

Dr. Mordechai Guri  
moti.guri@gmail.com

Matan Monitz  
mmonitz@gmail.com

Yisroel Mirsky  
yisroel@post.bgu.ac.il

Prof. Yuval Elovici  
elovici@inter.net.il

## Publications

M. Guri, M. Monitz, Y. Mirski, and Y. Elovici, "BitWhisper: Covert Signaling Channel between Air-Gapped Computers using Thermal Manipulations," 2015. arXiv:1503.07919.

## Demo video

<https://www.youtube.com/watch?v=EWRk51oB-1Y&t=15s>

## Goals

It has been assumed that the physical separation (air-gap) of computers provides a reliable level of security, such that should two adjacent computers become compromised, the covert exchange of data between them would be impossible. In this paper, we demonstrate BitWhisper, a method of bridging the air-gap between adjacent compromised computers by using their heat emissions and built-in thermal sensors to create a covert communication channel.

## Description

The BitWhisper method is unique in two respects: it supports bidirectional communication, and it requires no additional dedicated peripheral hardware. We provide experimental results based on implementation of a BitWhisper prototype, and examine the channel properties and limitations. Our experiments included different layouts, with computers positioned at varying distances from one another, and several sensor types and CPU configurations (e.g., virtual machines). Our discussion of signal modulation and communication protocols demonstrates how BitWhisper can be used for the exchange of data between two computers in a close proximity (at distance of 0-40 cm) at an effective rate of 1-8 bits per hour, a rate which makes it possible to infiltrate brief commands and exfiltrate small amount of data (e.g., passwords) over the covert channel.

# AirHopper: Bridging the Air-gap Between Isolated Networks and Mobile Phones Using Radio Frequencies

## Researchers

Dr. Mordechai Guri  
moti.guri@gmail.com

Matan Monitz  
mmonitz@gmail.com

Gabi Kedma  
gabikedma@hotmail.com

Assaf Kachlon  
assafka@post.bgu.ac.il

Prof. Yuval Elovici  
elovici@inter.net.il

## Publications

M. Guri, M. Monitz, and Y. Elovici, "Bridging the Air Gap between Isolated Networks and Mobile Phones in a Practical Cyber-Attack," ACM Transactions on Intelligent Systems and Technology (TIST), Special Issue: Cyber Security, Vol. 8, Issue 4, 2017.

G. Kedma, A. Kachlon and Y. Elovici, "AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies," 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE), Fajardo, PR, 2014.

## Demo video

<https://www.youtube.com/watch?v=20zTWiG1rM&t=20s>

## Goals

Information is the most critical asset of modern organizations, and accordingly coveted by adversaries. When highly sensitive data is involved, an organization may resort to air-gap isolation, in which there is no networking connection between the inner network and the external world. While infiltrating an air-gapped network has been proven feasible, data exfiltration from an air-gapped network is still considered to be one of the most challenging phases of an advanced cyber-attack. We present 'AirHopper', a bifurcated malware that bridges the air-gap between an isolated network and nearby infected mobile phones using FM signals.

## Description

While it is known that software can intentionally create radio emissions from a video display unit, this project was the first time that mobile phones were considered in an attack model as the intended receivers of maliciously crafted radio signals. We examine the 'AirHopper' attack model and its limitations, and discuss implementation considerations such as stealth and modulation methods. We tested AirHopper in an existing workplace at a typical office building and demonstrated how valuable textual and binary data, such as keylogging and files can be exfiltrated from physically isolated computer to mobile phones at a distance of 1-7 meters, with effective bandwidth of 13-60 Bps (Bytes per second).





# xLED: Covert Data Exfiltration from Air-gapped Networks via Router LEDs

## Researchers

Dr. Mordechai Guri  
moti.guri@gmail.com

Boris Zadov  
borisza@gmail.com

Andrey Daidakulov  
daidakul@post.bgu.ac.il

Prof. Yuval Elovici  
elovici@inter.net.il

## Publications

M. Guri, B. Zadov, A. Daidakulov, and Y. Elovici, "xLED: Covert Data Exfiltration from Air-Gapped Networks via Router LEDs," 2017. arXiv:1706.01140.

## Demo video

<https://www.youtube.com/watch?v=mSNt4h7EDKo>

## Goals

We demonstrate how attackers can covertly leak data (e.g., encryption keys, passwords and files) from highly secure or air-gapped networks via the row of status LEDs that exists in networking equipment such as LAN switches and routers.

## Description

Although it is known that some network equipment emanates optical signals correlated with the information being processed by the device ('side-channel'), intentionally controlling the status LEDs to carry any type of data ('covert-channel') has not been previously studied. We show how a malicious code is executed on the LAN switch or router, allowing full control of the status LEDs. Sensitive data can be encoded and modulated over the blinking of the LEDs. The generated signals can then be recorded by various types of remote cameras and optical sensors. We provide the technical background on the internal architecture of switches and routers (at both the hardware and software level) which enables this type of attack. We also present amplitude and frequency based modulation and encoding schemas, along with a simple transmission protocol. We implemented a prototype of an exfiltration malware and present a discuss of its design and implementation. We evaluated this method with a few routers and different types of LEDs. In addition, we tested various receivers including remote cameras, security cameras, smartphone cameras, and optical sensors, and addressed different detection and prevention countermeasures. Our experiment shows that sensitive data can be covertly leaked via the status LEDs of switches and routers at a bit rates of 10 bit/sec to more than 1Kbit/sec per LED.

# aIR-Jumper: Covert Air-gap Exfiltration/Infiltration via Security Cameras & Infrared

## Researchers

Dr. Mordechai Guri  
moti.guri@gmail.com

Dr. Dima Bykhovsky  
dmitrby@ac.sce.ac.il

Prof. Yuval Elovici  
elovici@inter.net.il

## Publications

M. Guri, D. Bykhovsky, and Y. Elovici, "aIR-Jumper: Covert Air-Gap Exfiltration/Infiltration via Security Cameras & Infrared," 2017. arXiv:1709.05742.

## Demo Videos

Infiltration: <https://www.youtube.com/watch?v=auoYKSzd0j4>

Exfiltration: <https://www.youtube.com/watch?v=om5fNqKjj2M>

## Goals

Infrared (IR) light is invisible to humans, but cameras are optically sensitive to this type of light. We show how attackers can use surveillance cameras and infrared light to establish bi-directional covert communication between the internal networks of organizations and remote attackers. We present two scenarios: exfiltration (leaking data out of the network) and infiltration (sending data into the network).

## Description

**Exfiltration:** Surveillance and security cameras are equipped with IR LEDs, which are used for night vision. In the exfiltration scenario, malware within the organization accesses the surveillance cameras across the local network and controls the IR illumination. Sensitive data such as PIN codes, passwords, and encryption keys are then modulated, encoded, and transmitted over the IR signals.

**Infiltration:** In an infiltration scenario, an attacker standing in a public area (e.g., in the street) uses IR LEDs to transmit hidden signals to the surveillance camera(s). Binary data such as command and control (C&C) and beacon messages are encoded on top of the IR signals.

The exfiltration and infiltration can be combined to establish bidirectional, 'air-gap' communication between the compromised network and the attacker. We implement a malware prototype and present data modulation schemas and a basic transmission protocol. Our evaluation of the covert channel shows that data can be covertly exfiltrated from an organization at a rate of 20 bit/sec per surveillance camera to a distance of tens of meters away. Data can be covertly infiltrated into an organization at a rate of over 100 bit/sec per surveillance camera from a distance of hundreds of meters to kilometers away.

# CYBER at BGV

Ben-Gurion University of the Negev



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



**Cyber@BGU [CBG]** serves as a shared research platform for the most innovative and technologically challenging projects, in partnership with various multi-national companies and governmental organizations. Situated in the Ben-Gurion Advanced Technologies Park in Beer-Sheva (Israel's Cyber Capital), CBG encompasses the Cyber Security Research Center, a joint initiative with the Israel National Cyber Bureau, and the Telekom Innovation Laboratories in partnership with Deutsche Telekom.

Core research under the Cyber@BGU umbrella includes IoT security; cyber for intelligent transportation; cyber for aviation; malware; AI-based cyber defense; fraud detection; blockchain; air-gap; network security; adversarial AI; machine learning and deep learning; and Big Data analysis for cyber security.

For up-to-date information on our research, go to: <https://cyber.bgu.ac.il/>

## Partnering for Growth





**Ben-Gurion University of the Negev** is the fastest growing research university in Israel. Just shy of its 50th anniversary, BGU is an agent of change, fulfilling the vision of David Ben-Gurion, Israel's legendary first prime minister, who envisaged the future of Israel emerging from the Negev in the south. From our three campuses in Beer-Sheva, Sede Boqer and Eilat, a vibrant, cutting-edge powerhouse in research and teaching has risen; the University now has around 20,000 students, 140,000 alumni and 4,000 faculty members in Engineering Sciences; Health Sciences; Natural Sciences; Humanities and Social Sciences; Business and Management; and Desert Studies.

BGU conducts major world-class research in biotechnology, arid zone research, conversion and inter-religious encounters, cyber security, energy, European politics and society, Hebrew literature, Jewish thought, nanotechnology, neuroscience, robotics, water and agriculture, and much more. Our special commitment to the community means that thousands of students take part in community outreach activities while pursuing academic excellence.

<http://www.bgu.ac.il>

**BGN Technologies** is the business and technology company of Ben-Gurion University of the Negev, Israel. Located in the heart of the University's Advanced Technologies Park, BGN Technologies is the driving force behind industry-academia collaborations, supporting the University's mission of cultivating a high-tech ecosystem within the Negev region.

With a track-record of over 100 startup companies, as well as partnerships in technology incubators and accelerators, BGN Technologies brings inventions from the labs to the market by fostering research collaborations and entrepreneurship among researchers and students.

During the past decade, BGN Technologies focused on creating long-term partnerships with dozens of companies, including multinationals such as: Deutsche Telekom, Dell-EMC, Lockheed Martin, IBM and PayPal, securing value and growth to the diverse ecosystem that surrounds BGU.

<http://in.bgu.ac.il/en/bgn/>

**CyberSpark - the Israeli Cyber Innovation Arena** in Beer-Sheva is a joint venture of the Israeli National Cyber Bureau in the Prime Minister's Office, the Beer-Sheva Municipality, Ben-Gurion University of the Negev and leading companies in the cybersecurity industry. This venture to support and develop the Beer-Sheva cyber ecosystem has been so successful that a recent Columbia University School of International and Public Affairs study examined the cyber "cluster" surrounding BGU as one of three successful case studies of "Cybersecurity as an Engine for Growth."

**CyberSpark Industry Initiative** was created by EMC, Jerusalem Venture Partners, Lockheed Martin and BGN Technologies, the University's technology transfer company, as a non-profit organization that will engage in the international promotion of the Beer-Sheva cyber hub and work to shape the next generation of cyber experts in the region. It has become the central coordinating body for joint cyber industry activities with government agencies, the IDF, the public and academia. The Initiative is formulating a multi-year business plan, leveraging the region's significant strengths and maximizing its potential in the field of cyber technology.

For more information please contact: Roni Zehavi, [roni@cyberspark.org.il](mailto:roni@cyberspark.org.il)

<http://cyberspark.org.il/>



Contact us for more information

Zafir Levy, Vice President  
Business Development  
Exact Sciences & Engineering  
BGN Technologies  
Tel: +972-52-2565715

[cyber@bgu.ac.il](mailto:cyber@bgu.ac.il)