Comparing the Effectivity of Planned Cyber Defense Controls in Order to Support the Selection Process

Paul Tavolato[1], Robert Luh[1,2], Sebastian Eresheim[1,2], Simon Gmeiner[1] and Sebastian Schrittwieser[1]
[1]*Faculty of Computer Science, Research Group Security and Privacy, University of Vienna, A-1090 Vienna, Austria*
[2]*Department of Computer Science, UAS St. Pölten, A-3100 St. Pölten, Austria*

Keywords: Security Management, Cyber Defense Measures, Security Control Assessment.

Abstract: Being able to compare the effectiveness of security controls on a sound quantitative basis would be of great benefit when it comes to decide which security controls should be implemented under given budget restrictions. This paper introduces a method for such comparisons based on a list of preventive defense actions and a list of attack actions, where the attack actions are supplemented by basic success probabilities; furthermore, a matrix showing the impact of the preventive defense actions on the success probabilities of attack actions is developed. Site specific characteristics are taken into account by the use of weights which must be defined by the security manager. Equipped with these tools a measure for the effectiveness of individual defense controls can be calculated. Comparing the measures provides valuable decision support in selecting defense controls to be implemented. A main focus lies on the easy applicability of the method to real-world situations. This is accomplished by incorporating information from several proven tactical and technical knowledge bases well established in the field.

1 INTRODUCTION

Every organization nowadays, may it be a small-scale business, a public service provider, or a multinational corporation, is confronted with an ever growing number of cyber-attacks. Hence, the implementation of an adequate cyber security management system is indispensable. The most widely accepted standards in this realm are the ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection (ISO/IEC, 2022) and the NIST Cybersecurity Framework (NIST, 2023). According to the ISO terms and definitions (ISO) cyber security is defined as the *protection of an IT-system from the attack or damage to its hardware, software or information, as well as from disruption or misdirection of the services it provides*. And Security management as the *process for design and monitoring of security policies, analysis, reporting and improvement of security*. And finally Information security management as *managing the preservation of confidentiality, integrity and availability of information*. It is part of the risk management of an enterprise and comprises:

the identification of an organization's assets (including people, buildings, machines, systems and information assets) the development, documentation implementation of policies and procedures for protecting assets.

In (Gold, 2004) we find a more detailed definition of Information Security Management as a *multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organizational, human-oriented and legal) in order to keep information in all its locations (within and outside the organization's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destroyed, free from threats*.

Information security management consists of the following main steps (Danzig, 1995):

1. Identifying information assets
2. Identifying potential threats, vulnerabilities, and impacts
3. Evaluating the risks
4. Deciding how to address or treat the risks, i.e., to avoid, mitigate, share, or accept them
5. Selecting appropriate security controls

Tavolato, P., Luh, R., Eresheim, S., Gmeiner, S. and Schrittwieser, S.
Comparing the Effectivity of Planned Cyber Defense Controls in Order to Support the Selection Process.
DOI: 10.5220/0012421800003648

In *Proceedings of the 10th International Conference on Information Systems Security and Privacy (ICISSP 2024)*, pages 211-218
ISBN: 978-989-758-683-5; ISSN: 2184-4356

6. Implementing the selected security controls
7. Monitoring the activities and making adjustments as necessary to address any issues, changes, or improvement opportunities

This paper focuses on step 5: the selection of appropriate security controls. As there are many possibly valuable security controls and their implementation is usually associated with considerable costs, security managers face the challenge of selecting the most effective controls under given budget restrictions. This requires a quantitative assessment of the effectiveness of individual security controls to provide a reliable basis for decision-making. Such a basis is necessary to select reasonable and effective security controls to be implemented (McCabe, 2007). This paper proposes such an assessment method based on information available from known and accepted sources of information security. To this end it breaks down security controls to elementary actions called defense actions and threats to attack actions. The main constituents of this method are:

- A list of defense actions
- A list of attack actions together with a success probability of each action
- An impact matrix describing the impact of an implemented defense action on the success probability of affected attack actions
- An overall measure to compare the influence of various defense actions on the collected success probabilities of the attack actions within the given environment of the system to be defended.

In order to be applicable in practice, the lists of defense actions and attack actions must be close to situations in practice. This is accomplished by taking information from several proven data sources such as STIX – Structured Threat Information eXpression language (MITRE Corporation, D), the APT kill chain by Hutchinson (Hutchins, Cloppert, & Amin, 2011), the CAPEC attack patterns – Common Attack Pattern Enumeration and Classification (MITRE Corporation, A), the MITRE ATT&CK – Adversarial Tactics, Techniques & Common Knowledge – attack and mitigation patterns (MITRE Corporation, B), the NIST SP 800-53 Countermeasures (Joint Task Force Transformation Initiative, 2015), and MITRE D3FEND (MITRE Corporation, C). The starting point of the defense and attack action lists is an adversarial cyber security game for threat assessment called PenQuest (Luh, Temper, Tjoa, Schrittwieser, & Janicke, 2019). In this role-playing game two players, the attacker and the defender, fight against each other in order to achieve their respective goal: The attacker has a predefined goal (violating one part of the CIA triangle) and the defender has a given infrastructure he wants to defend against attacks. The game is characterized by its high degree of practical relevance, mimicking real-life situations in cyber security as close as possible. The defense actions are attributed with success probabilities, which are based on published statistical data provided by the Cybersecurity and Infrastructure Security Agency (CISA, 2022).

The impact matrix, where the rows are the defense actions and the columns are the attack actions, defines for each defense action the amount of decrement of the success probability of the attack actions, if the defense action is implemented. The success probabilities of attack actions, which are not affected by the defense action under consideration remain unchanged.

The overall security measure of the system is defined as a weighted mean of all success probabilities. The weights must be provided by the security manager of the system – they reflect the site specific characteristics of the system. For example: if a system does not provide features to connect to the system by mobile devices, the weights for attack actions that aim at compromising mobile devices can be set to zero. This means that such attack actions will not have any influence on the overall measure.

Section 2 discusses related work, section 3 discusses the defense actions, section 4 the attack actions and in section 5 we describe the relationship between defense and attack actions, that is the influence that a defense action has on the success probabilities of attack actions, and the overall measure characterizing the effectivity of a defense measure. The last section summaries the assessment method and gives an outlook on future work.

2 RELATED WORK

There is some work on the assessment of security controls – but most of the papers deal with procedures to assess them after they have been implemented. These papers need not be considered, because the aim of this paper is the evaluation of the effectivity of security controls in the process of selecting appropriate controls, which happens before their implementation.

In (Johnson, 2020) the process of selecting security controls is subdivided into two separate procedures: first the selection of the baseline

security controls, which according to the risk analysis are indispensable, and second the selection of additional security controls. With respect to those additional controls he states that data from threat analysis "*...may affect organizational decisions regarding the selection of additional security controls, including the associated costs and benefits.*" But he does not give any advice on how this could be carried out.

Some research focusses on the decision process of selecting security controls like (Al-Safwani, Hassan, Katuk, 2014), (Al-Safwani, Fazea, Ibrahim (2018), (Otero, Tejay, Otero, & Ruiz-Torres, 2012) or others, but they lack either a detailed classification of defense and attack actions or they do not specify the origin of the data used.

The problem of collecting lists of attack actions is mostly described in the realm of threat modeling. Some valuable information can be found in the following papers – apart from the institutional sources already mentioned in the introduction: (Shostack, 2014), (Sidersky & Snyder, 20104), (Tarandach & Coles, 2020).

The relationship between attack and defense actions can be found in some institutional sources, for example in (CISA 2022). The mutual interdependence of defense and attack actions is incorporated in an extension of the well-known attack trees, the so-called attack-defense-trees (Kordy, Mauw, Radomorivic & Schweitzer 2014); some work on attack-defense-trees is concerned with quantitative evaluations (Aslanyan, Nielson, & Parker, 2016) and (Buldas, Gadyatskaya, Lenin, Mauw & Trujillo-Rasua 2020). Again, the source of the quantitative data the evaluation is based upon relies on subjective judgement and qualitative approaches only.

3 DEFENSE ACTIONS

As mentioned in the introduction a list of defense actions must be compiled that mirrors common cyber security practices. The basis for this list are known sources that contain established security controls that have stood the test in the field, mainly the MITRE D3FEND (MITRE Corporation, C) and the NIST SP 800-53 Countermeasures (Joint Task Force Transformation Initiative, 2015). There is quite a number of problems when attempting to compile such a list: there is no general standard of nomenclature and the delimitation of the defense actions from each other is not trivial as they might be on different abstraction levels.

The whole list compiled for this project contains 115 different defense actions which for reasons of clarity have been split into three categories:

1. Prevention actions
2. Detection actions
3. Response actions

Prevention actions are actions that are implemented to harden the system against attacks in general, to set up barriers in order to impede attack actions and to make the attacker's life harder (and more cost prohibitive). Examples of prevention actions are either of technical nature (e.g. encrypting data, establishing one-time passwords, validating input and so on) or they are of organizational nature (e.g. awareness trainings or incidence response trainings). The list contains 44 different prevention actions.

Detection actions are provided for detecting an attack. Examples of detection actions are analyzing traffic profiles, detecting remote terminals, analyzing resource use and the like. The delimitation between prevention and detection actions is sometimes blurry. The guiding rule was that a detection action always detects or reports an ongoing attack, while a prevention action generally tries to impede an attack or to even render it impossible. The list contains 48 different detection actions.

Response actions are defined as actions that mitigate the damage of an attack that already took place and was at least partially successful. Examples are disabling an account, blacklisting an address or a file or even shutting down the system. The list contains 23 response actions.

This paper is about the assessment of preventive actions only; detection actions and response actions will be dealt with in the future. The main goal is to evaluate the effectivity of each prevention action and hence provide a valuable decision basis for selecting security controls under given budget restrictions. A list of the 44 prevention actions can be found in the appendix.

4 ATTACK ACTIONS

In order to evaluate the impacts a prevention action has on the success probability of various attack actions, a list of attack actions together with a baseline of success probabilities is necessary. Again we use known and field-proven sources to construct the list, namely: the MITRE ATT&CK – Adversarial Tactics, Techniques & Common Knowledge (MITRE Corporation, B), the STIX –

Structured Threat Information eXpression language) (MITRE Corporation, D), the APT kill chain by Hutchinson (Hutchins, Cloppert, & Amin, 2011), and the CAPEC – Common Attack Pattern Enumeration and Classification attack patterns (MITRE Corporation, A).

For the sake of having a more structured list we classify the actions into three categories:

1. Reconnaissance actions
2. Actions for initial access
3. Execution actions

Reconnaissance actions are aimed at gathering information about the victim's system; they may be of technical or social engineering nature – sometimes there is no clear distinction. Examples for more technical actions are vulnerability scans or searching the victim's website; actions from the realm of social engineering are pharming or phishing. There are 15 reconnaissance actions in the list.

Actions for initial access are intended to get access to the victim's system via different means, for example by brute forcing a password, exploiting a vulnerability or maliciously manipulating inputs. There are 30 such actions in the list.

The largest group are actions for executing some payload on the victim's system, altogether 102 actions. They span a wide range of adversary activities including for example code injections, keylogging, stealing stored credentials, encrypting or destroying data, downloading malicious files, tracking mobile phone locations or many more.

The restriction to three categories is opposed to the CISA definition, which uses 11 groups (Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement. Collection, Command and Control, Exfiltration); such a distribution on 11 groups, however, leads to the disadvantage of attributions of an action to multiple groups. A list of the 147 attack actions can be found in the appendix.

Another important information needed for the intended purpose is a baseline success probability of each attack action. For this reliable data is not easily available. The Cybersecurity and Infrastructure Security Agency (CISA) issues a yearly report on "Risk and Vulnerability Assessments Results" (CISA 2022) which contains statistical data gathered from Risk and Vulnerability Assessments (RVA). Upon request, CISA identifies vulnerabilities that adversaries could potentially exploit to compromise security controls. CISA collects data in an on-site assessment and combines it with national threat information to provide customers with a tailored risk analysis report. The information gathered at these assessments is mapped to the MITRE ATT&CK™ TACTICS AND TECHNIQUES (MITRE Corporation, B) and for each technique a percentage is calculated representing the success rate for that technique across all RVA assessments of a year. In 2022 the data is based on 121 RVAs. We used this information as a starting point and complemented it accordingly where necessary.

5 IMPACT MATRIX DEFENSE–ATTACK ACTIONS

In order to assess the effectivity of a defense action another information is important: The impact of an implemented defense action on the success probability of an attack action. First, a decision has to be made, which attack action is influenced by a specific defense action. This information is available from the sources mentioned before, especially in CISA (2022) and also in (MITRE Corporation, B). In cases of doubt we decided in favor of an influence. As an example let's look at the attack action "Spearfishing": the following defense actions have a mitigating impact for this attack action: "Train Security Awareness", "Create Decoy Account" and "Validate Input". Another example: on the attack action "Keylogging", the following defense actions have a mitigating effect: "Encrypt Transmission", "Authenticate Messenger", "Check Driver Integrity", "Check Platform Integrity", "Check File Integrity", "Restrict Software Usage", "Limit Resource Utilization" and "Validate Input".

The impact an implemented defense action has on the success probability of an attack action is organized in the following groups:

1. Full annulation: the success probability of the attack action is reduced to 0.
2. Nearly full annulation: the success probability of the attack action is reduced to 10% of the baseline value.
3. Medium impact: the success probability of the attack action is reduced to 50% of the baseline value.
4. Small impact: the success probability of the attack action is reduced to 80 of the baseline value.
5. No impact: the success probability remains unchanged.

Reductions of success probabilities may add up: a second or third defense action aiming at the same attack action reduces the attack action's success probability even more. Of course, probabilities cannot have a value below 0.

For the afore mentioned examples we define the following impacts:

Table 1: Example of impact matrix.

	Spearfishing	**Keylogging**
Train Security Awareness	medium	no impact
Create Decoy Account	small	no impact
Validate Input	small	no impact
Encrypt Transmission	no impact	full annulation
Authenticate Messenger	no impact	nearly full annulation
Check Driver Integrity	no impact	medium
Check Platform Integrity	no impact	medium
Check File Integrity	no impact	small
Restrict Software Usage	no impact	small
Limit Resource Utilization	no impact	small
Validate Input	no impact	small

With the help of this matrix the effectiveness of a specific defense action or a set of defense actions can easily be calculated: it is represented by the overall reduction in the success probabilities of affected attack actions. Site specific features are incorporated into the method by means of a weighting of the attack actions. For each attack action the security manager of the system under consideration must decide on the relevance of each attack action within the environment under consideration. This information should be right at hand from the first three steps of information security management as defined in (Danzig 1995) and mentioned in the introduction: identifying assets, identifying potential threats, vulnerabilities, and impacts and risk evaluation. The success probabilities of the attack actions are multiplied by these weights. Some attack actions may be irrelevant in the environment under consideration and hence the corresponding attack actions can be given a weight of 0. Others might be of utter importance in that environment leading to a larger weight. Weight values are limited to the interval [0,2], meaning that the maximum weight doubles the importance of the attack action, while a value of 0 nullifies the action.

To compute the overall measure S the success probabilities of the attack actions are multiplied by the weights and the mean value of all weighted probabilities is calculated. Mind, that this is no more a probability as S might be larger than 1.

To compare the effectiveness of two defense actions (or sets of defense actions) d1 and d2, apply the row corresponding to d1 of the impact matrix to the success probabilities of all attack actions, which changes some of the probabilities; then compute S_{d1}. Do the same for d2 giving S_{d2}. Comparing S_{d1} to S_{d2} shows whether d1 or d2 has a more effective influence in the given environment: if $S_{d1} < S_{d2}$ then d1 must be preferred to d2 as it implies a lower overall risk.

6 METHOD SUMMARY AND FUTURE WORK

The goal of this proposal is to provide viable and realistic decision support for security managers facing the problem of assessing the effectiveness of specific defense controls (or sets thereof) before their implementation. Restricted budgets make such an assessment indispensable when trying to optimize expenditures. The method proposed here consists of the following steps (see Figure 1):

1. Make up site specific weights for all attack actions reflecting the importance of each attack action in the context of the system under consideration. This information should be available from the results of the risk analysis so far.
2. Choose some defense actions for comparison.
3. For each defense action calculate the values for all attack actions by multiplying the attack actions' success probabilities with the weights and compute the mean of these values. This gives the effectivity value of he defense action.
4. Compare the defense actions by these mean values: the lower the value, the more effective is the defense action.

With the suggested process security managers can compare the effectiveness of specific security controls. The key ingredients are the list of preventive defense actions and the list of attack actions. The attack actions are attributed with

success probabilities; finally there is a matrix relating the defense actions to the attack actions containing the impact of a specific defense action on the success probabilities of those attack actions affected by the defense action in question. The amount of reduction of success probabilities of a defense action signifies its effectiveness. Thus, different defense controls can be compared with respect to their effectiveness in tackling cyber-attacks in a given environment. Under given budget restrictions such assessment constitutes a valuable decision support for security managers.

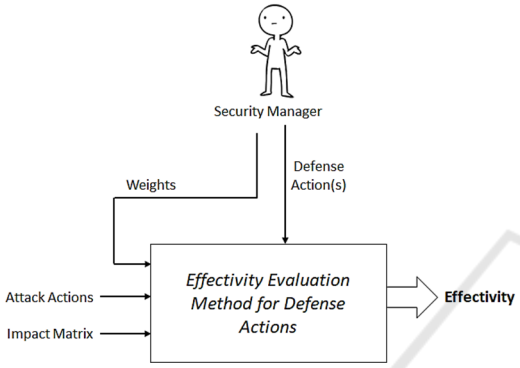

Figure 1: Method overview.

The main contributions of this paper are:

- A practical method to compare planned defense controls with respect to their effectiveness
- A consolidated list of preventive defense actions
- A consolidated list of attack actions together with a success probability for each action
- An impact matrix defining the amount of impact of a defense action on the relevant attack actions
- Integrating site-specific information into the method by means of a weighting of the attack actions

Future work will include fine-tuning the action lists: the prevention defense actions as well as the attack actions. The list of prevention actions is rather complete, but may need adjustment with respect to the abstraction level of some actions; furthermore, the definitions of each action may be improved to exclude misinterpretation. The list of attack actions so far only includes actions directly aimed at doing harm to the victim. The list could be augmented with so-called support actions; by support actions we mean actions that support the attacker's strategy without doing explicit harm to the victim system; these are actions for hiding effects of the attack from being detected by defense controls, such as removing log entries, hiding files that were created by the attack, suppressing execution warnings, downloading additional code and the like. Furthermore, the success probabilities of attack actions can be updated when new information is available. Another future work will be the integration of detection and response actions into the defense action list.

ACKNOWLEDGEMENT

This research was funded in whole, or in part, by the Austrian Science Fund (FWF) P 33656-N. For the purpose of open access, the author has applied a CC BY public copyright license to any Author Accepted Manuscript version arising from this submission.

REFERENCES

Al-Safwani, N., Hassan, S, Katuk, N. (2014). A Multiple Attribute Decision Making for Improving Information Security Control Assessment. International Journal of Computer Applications (0975 – 8887) Volume 89 – No.3, March 2014: pp 19-24

Al-Safwani, N., Fazea, Y., Ibrahim, H. (2018). ISCP: In-depth model for selecting critical security controls. Computers & Security, Volume 77, 2018, pp565-577. https://doi.org/10.1016/j.cose.2018.05.009.

Aslanyan, Z., Nielson, F., & Parker, D. (2016). Quantitative Verification and Synthesis of Attack-Defence Scenarios. IEEE 29th Computer Security Foundations Symposium, CSF 2016, (S. 105-119). doi:10.1109/CSF.2016.15

Buldas, A., Gadyatskaya, O., Lenin, A., Mauw, S., & Trujillo-Rasua, R. (2020). Attribute Evaluation on Attack Trees with Incomplete Information. Computers and Security 88/101630.

CISA (2022). FY22 Risk and Vulnerability Assessments (RVA) Results. https://www.cisa.gov/news-events/alerts/2023/07/26/ cisa-releases-analysis-fy22-risk-and-vulnerability-assessments

Danzig, Richard (1995). The big three: Our greatest security risks and how to address them. DTIC ADA421883

Gold, S (2004). Threats looming beyond the perimeter. Information Security Technical Report. 9 (4): 12–14. doi:10.1016/s1363-4127(04)00047-0.

Hutchins, E., Cloppert, M., & Amin, R. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Lead. Issues Inf. Warf. Secur. Res. 1/80.

ISO Online Browsing Platform. https://www.iso.org/obp/ui#home

ISO/IEC. ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection - Information security management systems. https://www.iso.org/standard/27001

Joint Task Force Transformation Initiative. (2015). SP 800-53 rev. 4. Recommended Security Controls for Federal Information Systems and Organizations. Gaithersburg.

Johnson. L. (2020). Security Controls Evaluation, Testing and Assessment Handbook. Second edition, Academic Press.

Kordy, B., Mauw, S., Radomorivic, S., & Schweitzer, P. (2014). Attack–Defense Trees. Journal of Logic and Computation, Volume 24/1, S. 55–87. Von http://logcom.oxfordjournals.org/cgi/reprint/exs029?

Luh, R., Temper, M., Tjoa, S., Schrittwieser, S., & Janicke, H. (2019). PenQuest: a gamified attacker/defender metamodel for cyber security assessment and education. Journal of Computer Virology and Hacking Techniques. doi:https://doi.org/10.1007/s11416-019-00342-x

McCabe, J. D. (2007). Network Analysis, Architecture, and Design. Morgan Kaufmann.

MITRE Corporation. (A). CAPEC—Common Attack Pattern Enumeration and Classification. https://capec.mitre.org/

MITRE Corporation. (B). MITRE ATT&CK. https://attack.mitre.org/

MITRE Corporation. (C). MITRE D3FEND. https://d3fend.mitre.org/resources/D3FEND.pdf

MITRE Corporation. (D). STIX—Structured Threat Information Expression | STIX Project Documentation. https://oasis-open.github.io/cti-documentation/

NIST Computer Security Resource Center (2023). The NIST Cybersecurity Framework 2.0. https://www.nist.gov/cyberframework

Otero, A.R., Tejay, G., Otero, L.D. & Ruiz-Torres, A.J. (2012). A fuzzy logic-based information security control assessment for organizations. 2012 IEEE Conference on Open Systems, Kuala Lumpur, Malaysia, 2012, pp. 1-6, doi: 10.1109/ICOS.2012.6417640.

Shostack, A. (2014). Threat Modeling: Designing for Security. Wiley.

Swiderski, F., & Snyder, W. (2004). Threat Modeling. Microsoft Press.

Tarandach, I., & Coles, M. J. (2020). Threat Modeling: A Practical Guide for Development Teams. O'Reilly.

APPENDIX

List of Defense Actions – Prevention

Check Exception Handler	Create Decoy Persona	Separation of Duties	Check File Integrity
Prevent Segment Execution	Publish Decoy Information	Least Privilege	Authenticate Bootloader
Randomize Start Address	Authenticate Transmission	Limit Logon Attempts	Least Functionality
Detect Segment Overwrite	Encrypt Transmission	Auto-Lock Session	Limit Info Disclosure
Remove Unneeded Code	Authenticate Messenger	Require Re-Authentication	Restrict Software Usage
Authenticate Pointer	Reroute Broadcast	Run Decoy Service	Restrict Hardware Usage
Verify Server Identity	Use Encrypted Tunnel	Run Decoy System	Restrict Software Install
Multi-Factor Authentication	Encrypt Data	Run Decoy Network	Limit Resource Utilization
One-Time Password	Dispose Data	Place Decoy Session Token	Validate Input
Remove User Permissions	Check Driver Integrity	Create Decoy Account	Train Security Awareness
Restrict User Accounts	Check Platform Integrity	Place Decoy Data	Train Security Response

List of Attack Actions – Reconnaissance

Hijack External Account	Collect Org Information	Collect Device Information	Search Victim Website
Collect Net Information	Buy Information	Collect User Information	Pharming
Vulnerability Scan	Search Open Source Info	Search Technical Info	Pretexting
Discovery Scan	Scan System	Phishing	

List of Attack Actions – Initial Access

Drive-by Compromise	Abuse Password Recovery	Mobile: Attack via USB	Hijack Connection
Remote Access	Exploit Bug (Access)	Mobile: Install Evil App	Denial of Service
Misuse Remote Access App	Brute Force	Mobile: Abuse PC Link	Append Malicious App
Remote Service Connect	Use Hash Authentication	Mobile: Abuse WiFi	Append Malicious Doc
Abuse Auto-Installer	Manipulate Shared File	Mobile: Manipulate Settings	Exploit Bug (Evasion)
Provide Malicious Update	Install Hardware	Mobile: Bypass Lockscreen	Spearphishing
Manipulate Input	Malicious USB Drive	Network Denial of Service	Request Screen Control
Impersonate Login Prompt	Compromise Supply Chain		

List of Attack Actions – Execution

Record Microphone	Steal Stored Passwords	Wipe Disk	Mobile: Service Login
Read User Bookmarks	Check Permissions	Compromise Firmware	Mobile: Root/Jailbreak
Install Browser Plugin	Cloud: Steal Token	Mobile: Steal Data	Sniffing
Steal Clipboard Data	Steal Cookie	Android: Read Notification	Man in the Middle
Manipulate System App	Steal Authentication Ticket	Mobile: Scan Apps	Search Network Services
Manipulate Website	Intercept OTP	Android: Broadcasts	Search Network Shares
Hijack App Execution	Steal Unsecured Passwords	Mobile: Steal SMS	Read Net Configuration
Cloud: Add Container	Destroy System Data	Android: Billing Fraud	Check Net Connections
Take Screenshot	Destroy User Data	Mobile: Lock Device	Check App Windows
Buffer Overflow	Encrypt System Data	Mobile: Eavesdropping	Cloud: Scan Infrastructure
Manipulate Pointer	Encrypt User Data	Mobile: Control SMS	Cloud: Read Dashboard
Code Injection	Manipulate System Data	Android: Force Foreground	Cloud: Search Service
Manipulate Server App	Manipulate User Data	Mobile: Activity Fraud	Manipulate Boot Process
Manipulate System Service	Steal Configuration Data	Mobile: Fake Input Prompt	Scan Registry
Record Webcam	Steal Local Data	Mobile: Jamming	Hijack Resources
Abuse Windows Mgmt App	Steal Network Share Data	Mobile: Track Location	Read System Info
Manipulate Domain Policy	Steal Correspondence	Android: Manipulate Cache	Check System Services
Exploit Bug (Execution)	Search Files	Mobile: Manipulate Startup	Shut Down
Exploit Bug (Elevation)	Auto-Start Program	Android: Run Native Code	Manipulate App
Exploit Bug (Credentials)	Auto-Start Script	Mobile: Steal Cloud Backup	Inter-Process Comm.
Lock Account	Run Command	Mobile: Remote Wipe	Auto-Start Office File
Manipulate Account	Run Triggered Command	Mobile: Rogue Cell Tower	Check Processes
Create Account	Run Program Function	Mobile: Rogue Access Point	Process Injection
Steal Stored Credentials	Schedule Task	Mobile: Swap SIM Card	Man in the Browser
Auto-Logon	Stop Service	Mobile: Read Device Info	Request User Execution
Keylogging	Load Evil Library		