cloud security alliance®

Switzerland Chapter

Cyber Threat Psychology Research Project

ISACA AHS Round Table 5/25
Zürich, 07 October 2025

Considerations

A cyber attack involves multiple actors whose motivations, thinking, behaviours and experiences often are going back into early childhood of hackers, victims, intermediaries.

Congruency of motivations between the attacker and the target victims often facilitates the attack.

The congruency may not be apparent at all, rather, there may be subconscious biases influencing.

Psychological factors such as pride, frustration, effects from mobbing, lack of recognition, neglect, geniality (either not understood or not accepted) can be very strong drivers on either side.

For a cyber attack to succeed, the transmission mechanisms between the hackers and their victims and the communication aspects are of equally relevant importance.

Awareness and communication can significantly help to intercept tendencies to develop hacktivism, and on the other hand, for others to become more alert to signs of people developing patterns which may indicate them derailing into hacktivist approaches.

Research Outline

Focus areas are :

- The psychological motivations of attackers (the “Supply Side”).
- Their origins from personal conditions, social context and behaviour.
- Ways of interception at the “Supply Side”: identify developing personal conditions which may lead persons to succumb to influences or personal conditions to become hackers.
- Potential approaches how to influence behaviours of attackers to turn them into positive constructive contribution rather than negative harmful destruction.
- The transmission mechanisms: subversion, deception, poisoning.
- Potential behavioural change at “Receiver Side” to understand the background of hacktivism, to develop and to apply communication, social, emotional awareness and better detection and response.
- Changing the incentive patterns and mindsets of both the “Supply Side “ and the “Receiver Side” to reduce attacks and impact.

Objectives

Develop education, awareness and communication programs at multiple levels:

- Empower individuals to cultivate curiosity, social / emotional awareness and to spread security-conscious behaviour.
- Instill mischievous vigilance to help potential victims to recognize and resist hacking attempts, by understanding and reducing psychological and social attack vectors.
- Sharpen mindset of all to be aware of their digital oversharing which facilitates exploitation and social engineering.
- Raising public awareness to identify individuals in their personal environment who may be susceptible to drift off track due to personal conditions which may result in them developing hacking tendencies.
- Providing guidance and support to help such individuals to shift perspectives before crossing ethical lines.
- Advising organizational leadership on how to foster a security-conscious culture that enhances resilience against hacking activities.
- Strengthening the human firewall by understanding how people feel, are impacted, think, share, act and react.
- Develop communication programs to equip individuals to detect manipulation tactics, fostering critical thinking in online interactions, psychological resilience, and strategic defense mechanisms.

Tune in … A typical Attack Constellation

Considerations: Setting the scene

- A service provider has developed a cutting edge AI based SaaS application which helps customers to save much time in processing customer requests.
- The SaaS application is promoted via events, Google Ads, Social Media posts and attracts lots of attention.
- The service provider is a small company, 10 partners who cooperate closely and share the spirit.
- Development of the SaaS application is rapid and agile with frequent feature releases in response to customer requirements.
- Partners in the service provider know each other since long, share duties and information, and all have development, support and administration privileges to provide fast and responsive customer service and release management.
- The SaaS application earns recognition and is awarded a prize for innovativeness.
- The CEO of the service provider is invited to the awards ceremony, he shares the success on LinkedIn, many congratulations, invitations and connections follow.

Tune in … A typical Attack Constellation

Considerations: Know whom you can trust …

- Several LinkedIn connections interact intensively with the CEO and his partners, talking about the cool application, how it helps other companies, what makes it so efficient, which libraries it uses. Some contacts suggest further improvements.
- One of the contacts is a former partner of the service provider's team who initially contributed with his genius ideas but later had been dismissed after severe concerns about his conduct. He has not found a new position and after long time of frustration, social decay and poverty, found good friends and inspirational recognition in darknet fora.
- The disgruntled former partner teams up with his new friends to plan an attack destroying his former partners' achievements which he thinks they owe to him mostly.
- The evil teamsters use fake accounts, hail the CEO and his partners, lull them into passing information about the SaaS application's architecture, the libraries, the AI models, the data it uses etc., and then poison both the data and the AI models.
- With the poisoned models and poisoned data, customers are given wrong answers.
- With the socially engineered proximity, identities and accounts are taken over thanks to phished information.

Tune in … A typical Attack Constellation

Lessons from the case:

- Disgruntled staff or partners may turn into enemies because of
    - Lost employment
    - Lost social stance
    - Pride having been violated
    - Genius (whether true or just imagined) not having been appreciated
- People may after falling seek orientation and support from seemingly strong and super-hero friends.
- Revenge turns into criminal energy which comes in admiration disguise.
- Both sides feel flattered…
- Which results in an easy to exploit situation where both the Supply Side and the Receiving Side feel good!
- Interception would have to act much earlier, by monitoring and detecting and counteracting critical behaviours.

CSA Cyber Threat Psychology Research: Approach

Research into Cyber Threat Psychology is aiming at:

1. Identifying personal conditions which foster the development of behaviours ultimately being deployed to hacktivism:
    a) Shyness, often correlated with fragility, not being able to show their skills or being exploited
    b) Genius: Super intelligent but often at the same time unable to form social relations
    c) One-sided excellence: A form of genius, people are excellent at one particular aspect e.g. logics, but lack most other
    d) Isolation: Often a result of the combination of the above, but people may still want to relate, interact, show their skills
    e) Social media consumption: Exploitation of soft spots, frustrations, lead people into the arms of seeming idols
    f) Unrecognised strengths: People have special strengths but cannot make them apparent, or are not allowed to develop them, or are not supported
    g) Frustration from what people may consider unfair treatment at school or at job
    h) Disgruntlement after dismissal, or after not being considered for promotion, or for personal reasons in relationships
    i) Ideology: often in combination with one or several of the above, also for religious reasons
    j) ...

CSA Cyber Threat Psychology Research: Approach

Research into Cyber Threat Psychology is aiming at:

2. Identifying social context conditions which foster the development of behaviours ultimately being deployed to hacktivism:
    a) Neglect: Family, friends, lovers, colleagues
    b) Lack of appreciation: People who are not socially shining, who do not look great, who may have an injury, handicap…
    c) Bullying: Showing others they are capable in another way, to strike back
    d) Mobbing: Triggering disgruntlement, hate and revenge
    e) Skills not being recognized: People who could excel but school / job does not allow them
    f) The power of words: Soft people may succumb to teasers and demagogues, super-hero types, shiny evils
    g) Social environment: Surrounded by people whose motivations and drivers may be evil, converging onto or resorting to them because of one or several of the above
    h) Political system: Fostering a culture of hacktivism, rewarding attacks, spreading dis-information, inspiring hate
    i) Chance equality: Bright minds who may not know how to get a chance to shine or develop
    j) …

CSA Cyber Threat Psychology Research: Approach

Research into Cyber Threat Psychology is aiming at:

3. Analysing the transmission mechanisms at the “Supply Side”: most people in the same constellation don’t develop the negative mindset of hackers. What are combinations of factors resulting in evil mentality?
    a) Soft personality, shyness
    b) Frustration, lack of recognition
    c) Suffering from colleagues, partners, friends, job
    d) Want to shine and do well, be accepted and recognised
    e) Want to break out from lack of recognition, lack of appreciation, pressure … search for alternatives
    f) Meet shiny people who appear strong, convincing, and give the soft people seemingly what they crave for
    g) Even more: make them feel needed, indispensable, important, recognised
    h) Lack of economic perspectives and at the same time political system rewarding patriotism
    i) Lack of personal environment which can detect any of the above and support in changing perspective
    j) Mental instability
    k) Feeling of being left out

CSA Cyber Threat Psychology Research: Approach

Research into Cyber Threat Psychology is aiming at:

4. Identifying potential interception points and mechanisms “Supply Side”:
    a) Which of the above conditions and transmission mechanisms are suitable to interfere with?
    b) What possible interference patterns and approaches exist and how can these be tuned to achieve positive outcome?
    c) Longer term approaches to impact change in the conditions to prevent them from fertilising hacktivism mindset.
    d) “Social engineering”: target potential or actual Hackers and their social environment via the conditions and transmission mechanisms identified in this research project, to approach them and effect a mindset change.
    e) Influencing in a positive sense before Hackers turn into evil: recognise their potential early, identify situations in which people may turn from despair to criminality, foster a culture of providing a safe harbour and offering other perspectives.
    f) Often, the environment of those who may turn into a hacker career sees signs much earlier before the actual tipping point: inform the general public about such signs and encourage them to watch and interfere or seek support.
    g) Offer and broadly communicate programs which are publicly accessible and which address and are appealing to people with such special situations or skills.
    h) Offer a scheme of recognition which is as strong and incentivising as the Dark Net Recognition.

CSA Cyber Threat Psychology Research: Approach

Research into Cyber Threat Psychology is aiming at (continued):

5. Analysing and identifying interception points in the transmission mechanisms between the "Supply Side" and the "receiver side":
   Congruency of "Supply Side" and "Receiver Side" motivators e.g. craving for appreciation

   a) Undermining with subversion: Get closer to the targets: intrusion into social channels, connecting, posing, praising, applauding, establishing credibility, establishing trust, collecting information, beginning to subtly seed information.

   b) Influencing with deception: working actively on the targets, leverage trust established to influence with own information which may include partial misinformation, throw baits in disguise in the context of the established trust, engage even more and foster action by the targets to reveal more critical information, etc.

   c) Acting with poisoning: "Psychology as a Weapon" and "Code as a Weapon": targeting the broad public or specific important / highly respected individuals with psychological means to poison their opinion and to leverage them thereafter as opinion leaders to achieve wide spread poisoning. Misuse the trust established and the information gathered during the undermining and influencing phases, to weaponise and intrude into protected environments via identity and authentication hijacking, misuse identity and their credibility to intrude into trusted news feeds, fora, social media to further inject and spread poisoned information to poison the receiving society.

Communicate: Any of these can be leveraged to detect, counter-influence, intercept, neutralise, turn around.

CSA Cyber Threat Psychology Research: Approach

Research into Cyber Threat Psychology is aiming at (continued):

6. Identify action points on the "Receiver Side":
    a) All: educate to overcome the lack of understanding of exposure to cyber attacks, social engineering, indirect exposure via careless information sharing or unconscious biases of trust, and their transmission mechanisms.
    b) All: Behaviour change: how to apply curiosity and social / emotional awareness and turn it into mischievous vigilance to prevent being caught by hacking.
    c) Private Individuals: awareness activities to help identifying potential persons in the personal environment who could become susceptible to developing into hacktivism, and to coach or encourage them to change mindset or route, or to offer them alternatives, seek programs offered, outside support.
    d) Society and Communities: How does a state's society, a community or a group respond to the communication received via the transmission channels, in particular to the subversion, deception and poisoning triad?
    Can this be improved, sharpened, immunised by appropriate awareness and information / education campaigns?
    How can state / community leadership impact and positively influence this?
    e) Corporates: Top Management culture and behaviours exemplarily demonstrated.
    f) Corporates: Organisational culture change: modifying processes, incentives and organisational mindset.
    g) Corporates: All staff: Develop psychological, social and emotional awareness.

What do we want to deliver

Communication and awareness:

Design programs of communication:

- Content attuned to appeal to, attract and make think those who are on the “Supply Side”
- Active communication in fora, schools, universities, internet groups, social media, darknet channels
- Public programs to inform, raise awareness, develop understanding of such constellations, to:
    - Sharpen awareness and to sensitise people both for their own benefit not to fall prey so easily of attacks
    - Spot potential candidates on the “Supply Side”
    - Know about where to go for support and guidance
    - Know about transmission mechanisms employed, in particular when facing external state sponsored psychological interference
    - Know where to look for alternative, neutral or non-manipulated information, to be able to contrast potential attempts of state sponsored undermining, deception or poisoning

What we will not be able to change

State pressure and state sponsored hacktivism:

- Autocratic governments will always want to influence other nations. To counteract these attempts, public awareness of the transmission channels and the mechanisms of psychology as a weapon are critical and must be communicated actively and though many channels including social media reaching those who are usually not monitoring official information channels.
- Leverage psychology as a benign tool not weapon, to create constructive awareness.
- Train the general public to apply mischievous vigilance in any information they consume, to question, check, compare, seek alternatives.