Social Threats Modelling with *i**

Lin Liu[1] Eric Yu[2] Gul Jabeen[1]
[1]School of Software, Tsinghua University, Beijing, China
[2]School of Information, University of Toronto, Toronto, Canada

Understand the Social Perspectives of Security and Privacy is critical!

A recent phone scam tragedy…

Scammers know certain facts about you

- Name, phone number, address
- Citizenship id, bank account number…

A million messages sent per day from a base station in Anxi County, Fujian at a busiest time…

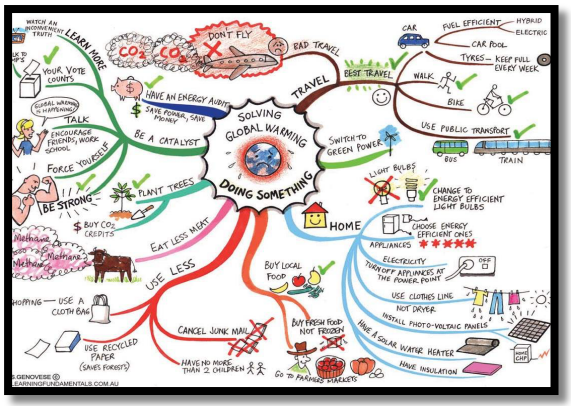
Scammers' identities, banks accounts remain untraceable…

The scammers were caught now, how to avoid such tragedies from happening again?

RE Provides Problem-Oriented Analysis

Provides concepts, models, processes, specifications for design and auditing…

- What is the problems and objective?
- Who is involved? Who are the attackers?
- Why they attack? What they gain?
- How they attack? When and where?
- What to protect?
- How to counteract?



Language	Approach	Focus
Goal-oriented	NFR	Software
	Secure i*	Organization; Software
	Secure Tropos	Organization; Software
	SI*	Organization; Software
	Obstacle/Anti-goal	Software
UML-based	Misuse Cases	Software
	UMLsec	Software; Infrastructure
	SecureUML	Software
Problem frame-based	Abuse Frame	Machine
	SEPP	Machine
	SREF	Machine

Coverage of the Universe (by Tong Li, et al.)

Language	Approach	Threat	Multistage attack
Goal-oriented	NFR	--	--
	Secure i*	√	√
	Secure Tropos	√	√
	SI*	--	--
	i* security modelling	√	√
	Obstacle/Anti-goal	√	√
UML-based	Misuse Cases	√	--
	UMLsec	√	--
	SecureUML	--	--
Problem frame-based	Abuse Frame	√	--
	SEPP	√	--
	SREF	√	--

Threat Analysis support (by Tong Li, et al.)

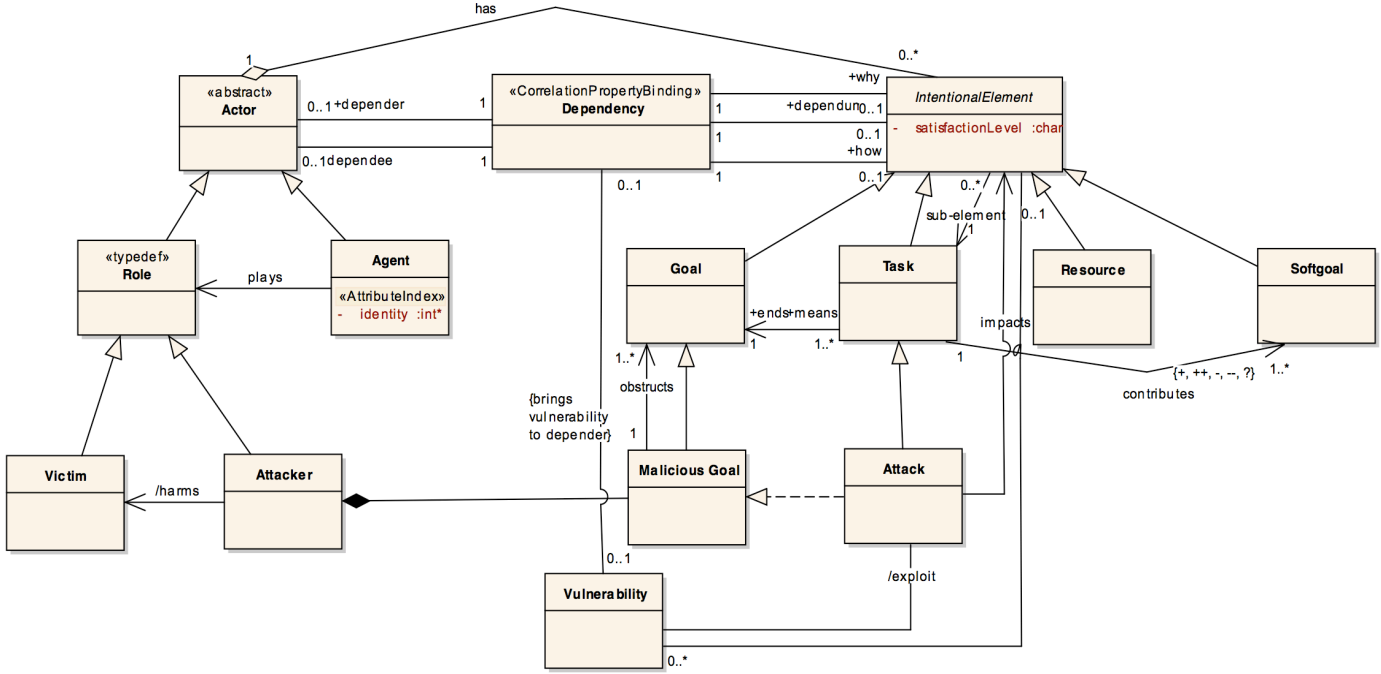
Knowledge Support (by Tong Li, et al.)

Language	Approach	Reuse	Source	Tool support
)	NFR	taxonomy	literature	applying taxonomy
Goal-oriented	Secure i*	--	--	--
	Secure Tropos	security patterns	four patterns	guideline
	SI*	--	--	--
	i* security modelling	vulnerability	CVE/CWE	--
	Obstacle/Anti-goal	--	--	--
UML-based	Misuse Cases	misuse cases	literature	guideline
	UMLsec	--	--	--
	SecureUML	--	--	--
Problem frame-based	Abuse Frame	abuse frame	literature	--
	SEPP	SPF/CSPF	three frames	guideline
	SREF	--	--	--

Motivation

- Security incidents lead to loss or disruptions of an organisation's operations, services or functions, or reductions in the quality of the expected services.
- For any security incident, there is an individual or a group of attackers, conducting the attack action, towards one or many victims.
- The two sides are played by social actors, with certain social positions, protecting or obstructing a given operations, services functions with certain techniques.
- In this paper, we propose a meta-model that aims to capture the act of attackers and the counter-act of the victims using social concepts in *i**. Such act vs. counteract, attack vs. protection situation is inherently socio-technical.
- By compensating existing tactical analytic frameworks on security, an important dimension of the problem space is tackled, which leads to the identification of effective solutions systematically that are otherwise by coincidence.

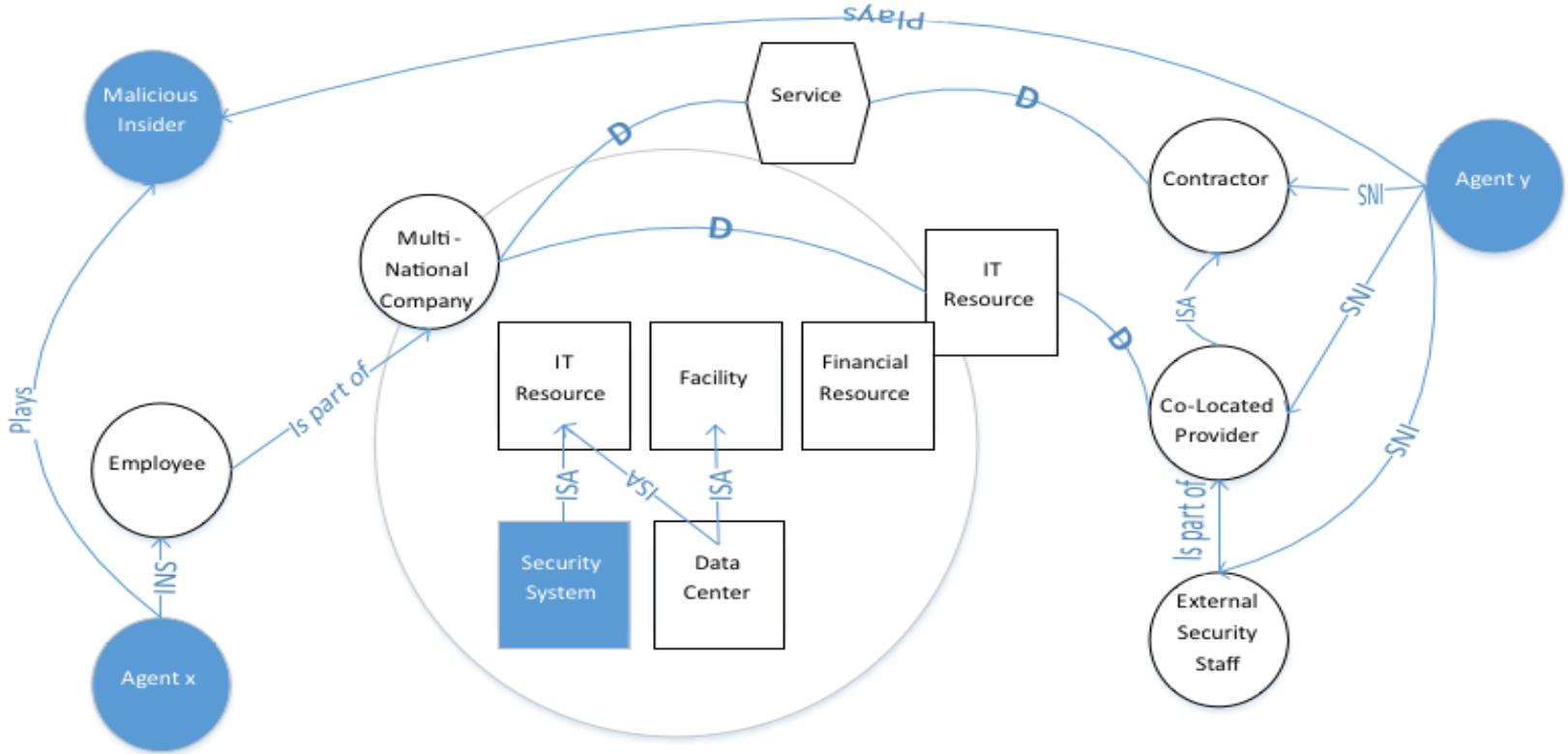
Meta-model of cyber security from an actor's viewpoint



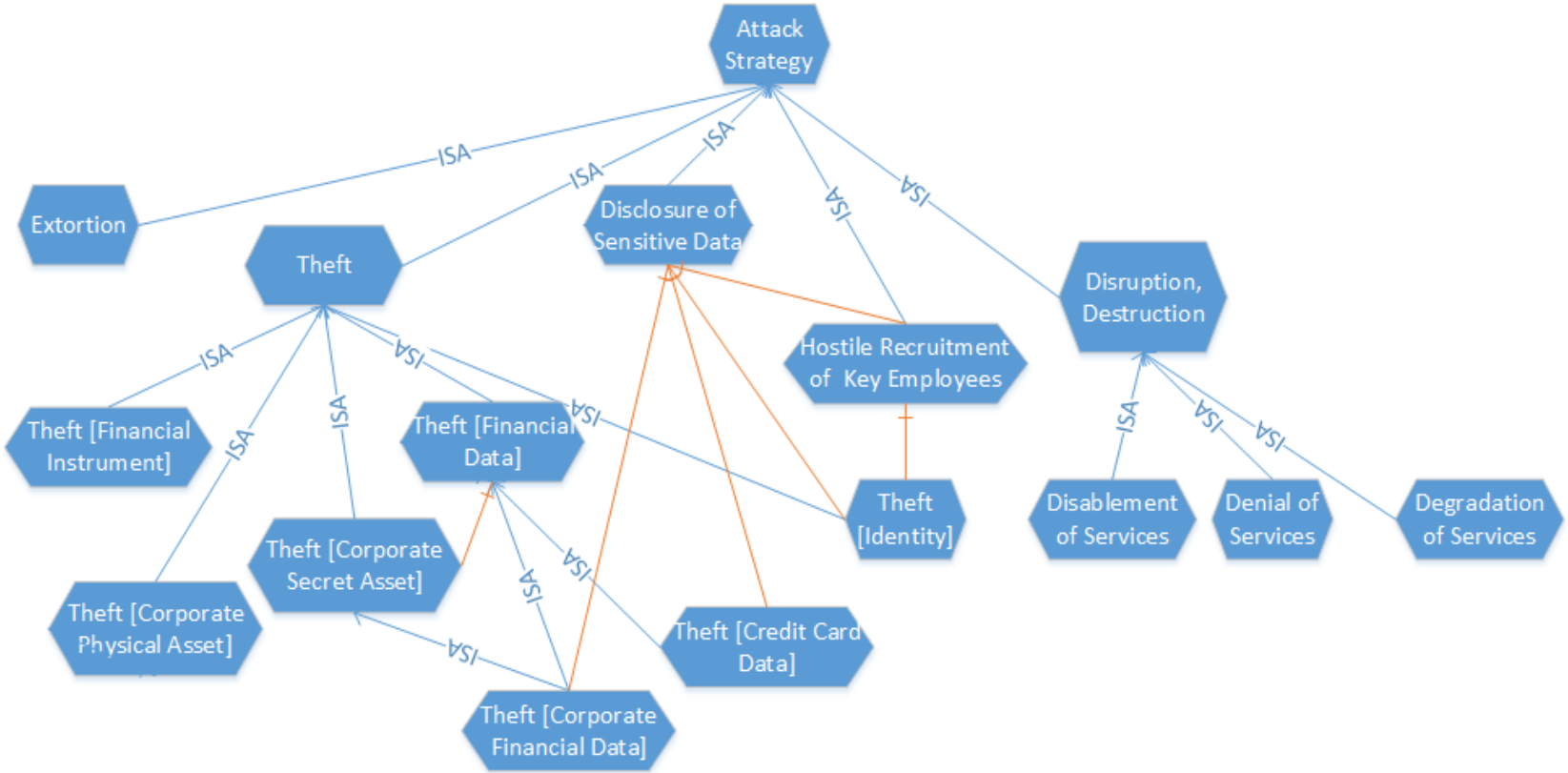
Use Case I: Corporate Information Security Threat

- A multi-national company with multiple datacenters, office facilities, and international business activity. Offices and data centers are located in the US, Europe, APAC. Some facilities are in countries with conflict of interests. Employees include citizens across all locations. Some data centers are hosted by a co-location provider with external security staff. Turnover of staff is within normal ranges. There are active use of contractors and other external partners, and a large number of deployed security systems, sensors.
- Information Security systems includes:
- Access control through directory, but large number of services that are not integrated;
- Basic endpoint security systems for most servers and laptops; Firewalls;
- Intrusion Detection System/Intrusion Prevention System (IDS/IPS);
- Security Information and Event Management (SIEM);
- Systems monitoring; Physical Security systems.
- Basic physical access control:
- Video monitoring of sensitive areas; Intrusion detection; Commercial fire alarms and suppression;
- Notification/alerting for critical events (through SMS, email, etc.)
- On call staff includes skeletal 24/7-support team, some on-call staff for escalation, External guards.

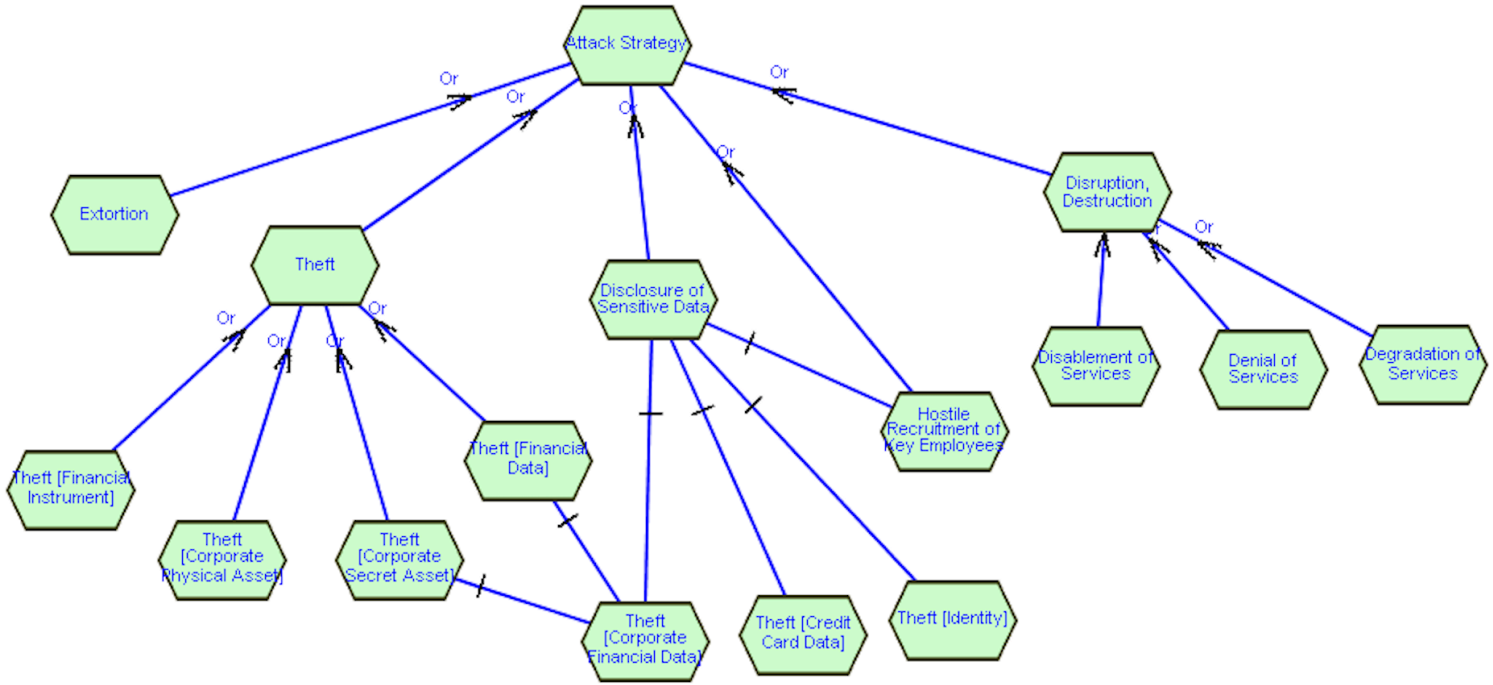
Use Case I: Corporate Information Security Threat



Modelling Attack Strategies using Classifications and Compositions



Modelling Attack Strategies using Task Decomposition



Potential adversaries

- Cyber criminals, including organized crime (domestic and foreign);
- Competitors;
- Malicious Insiders: Disgruntled employees and contractors;
- Hostile Investors: Potential corporate or individual acquirers of company;
- Nation state adversaries (unlikely, unless company engages in critical infrastructure or national defense, etc.);
- Terrorist Organizations.

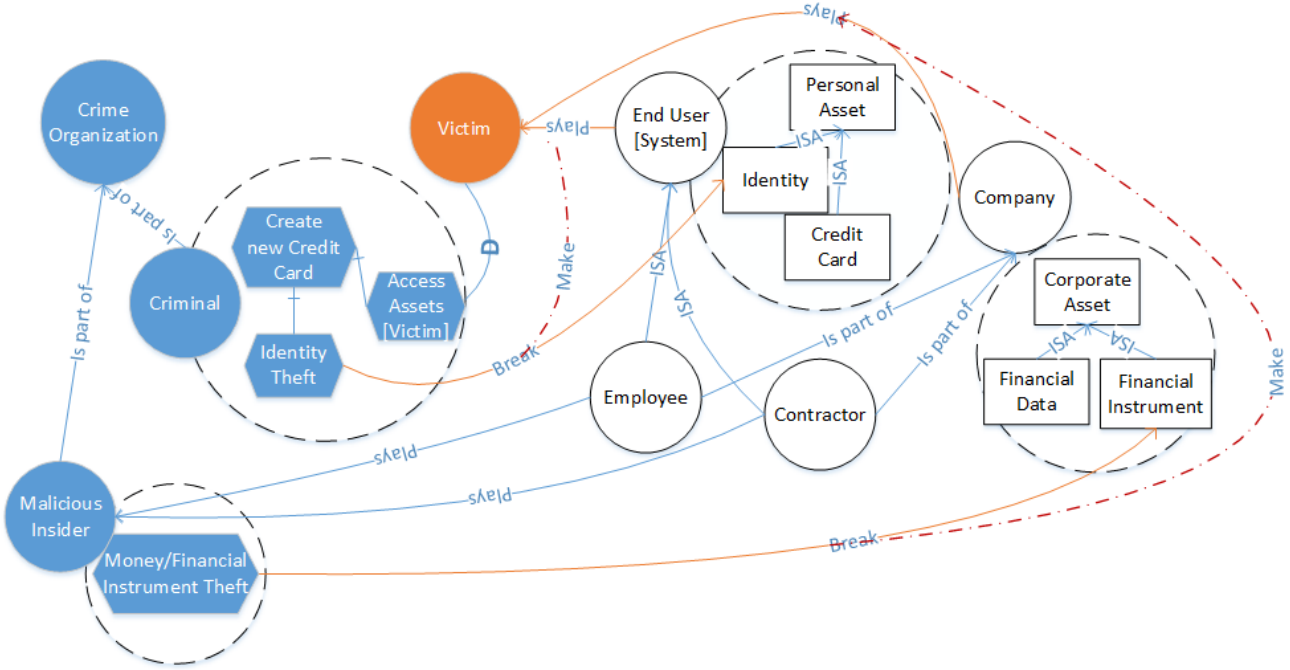
Potential motivation of adversaries

- Until attack is seen from the view of motivation for the criminals themselves, efforts to battle it will not yield their full promise.
- Cyber criminals are driven by time-honored motivations. Spotting these motivations could be an essential key to find a holistic solution.
- Not much research has looked into this important aspect of threats classification.

Main Strategies in the example case

- Identity Theft: the attacker attacks the end user systems or the corporate assets to obtain the identities of primarily the end users.
- Financial Data Theft: the attackers obtain sensitive financial information about end-users or other entities from corporate assets.
- Extortion/Ransom: the attacker obtains the ability to affect corporate assets negatively (e.g. through denial, destruction, disruption, degradation, distortion, data exfiltration, etc.) and blackmail the company. The company pays a ransom to avoid negative consequences.
- Money/Financial Instrument Theft: this is traditional direct theft of money, or similar financial instruments that can immediately be sold.

Strategic Rationale Modelling of the Attackers in Financial Gain Scenario



Formalisms

```
For ALL x in Actor, y in Resource, z in Attack,
Role-Play (Attacker, x) AND HAS-ACCESS(x, y) AND COMMIT(x, z)
=> Exist x' in Actor, Role-Play( Victim, x') AND LOSS (x', y, z);
For ALL x in Actor, y in Resource,
WithinBoundary(x, y) => HAS-ACCESS(x, y);
For ALL x in Actor, y, y' in Resource,
WithinBoundary(x, y) AND ISA(y, y') => WithinBoundary(x, y')  ;
For ALL x, x' in Actor, y in Resource,
WithinBoundary(x, y) AND (ISA(x, x') OR IS-Part-Of(x, x'))   =>
WithinBoundary(x', y)
For ALL x in Actor, z in Attack,
COMMIT(x, z) => WithinBoundary(x, z)
```

An Example Query

Given x, x’ in Actor, z in Attack,

if Role-Play (Attacker, x) AND HAS-ACCESS(x, Identity(x’)) AND COMMIT(x, z)

What will happen? By applying rule 1, 2, 5, we can derive the following result:

Role-Play(Victim, x’) AND { For All y in Resource, WithinBoundary(x’, y) => LOSS(x’, y, z)}.

Use Case II: Ransomware Threats Modeling

What ransomware is?

How do It effect the host system?

How it propagate itself?

How to detect it.

What are the vulnerabilities In the system?

What countermeasures should be taken by user to protect himself?

What ransomware is?

- A ransomware is the new form of cybercrime.
- Ransomware victimizes Internet users by
  - Hijacking user files
  - Deleting files from the system.
  - encrypting files
  - Demanding payment in exchange for the decryption key.

How do It effect the host system?

- Ransomeware always tries to grab control over the victim's files or computer until the victim agrees to the attacker's demands
- It searches different file extension such as .txt, .doc, .rft, .ppt, .chm, .cpp, .asm, .db, .db1, .dbx, .cgi, .dsw, .gzip, .zip, .jpg, .key, etc.
- Encrypt the data file of the user by using malicious code.
- Malicious code should be deleted after encrypting the files.
- Hide the files of system
- Generate Static Pop up menus in to the system which cannot be removed from the system

How it propagate itself?

The ransomware propagate itself in to the system by following ways.

- Email propagation
- Web files downloading
- External device propagation

How to detect it?

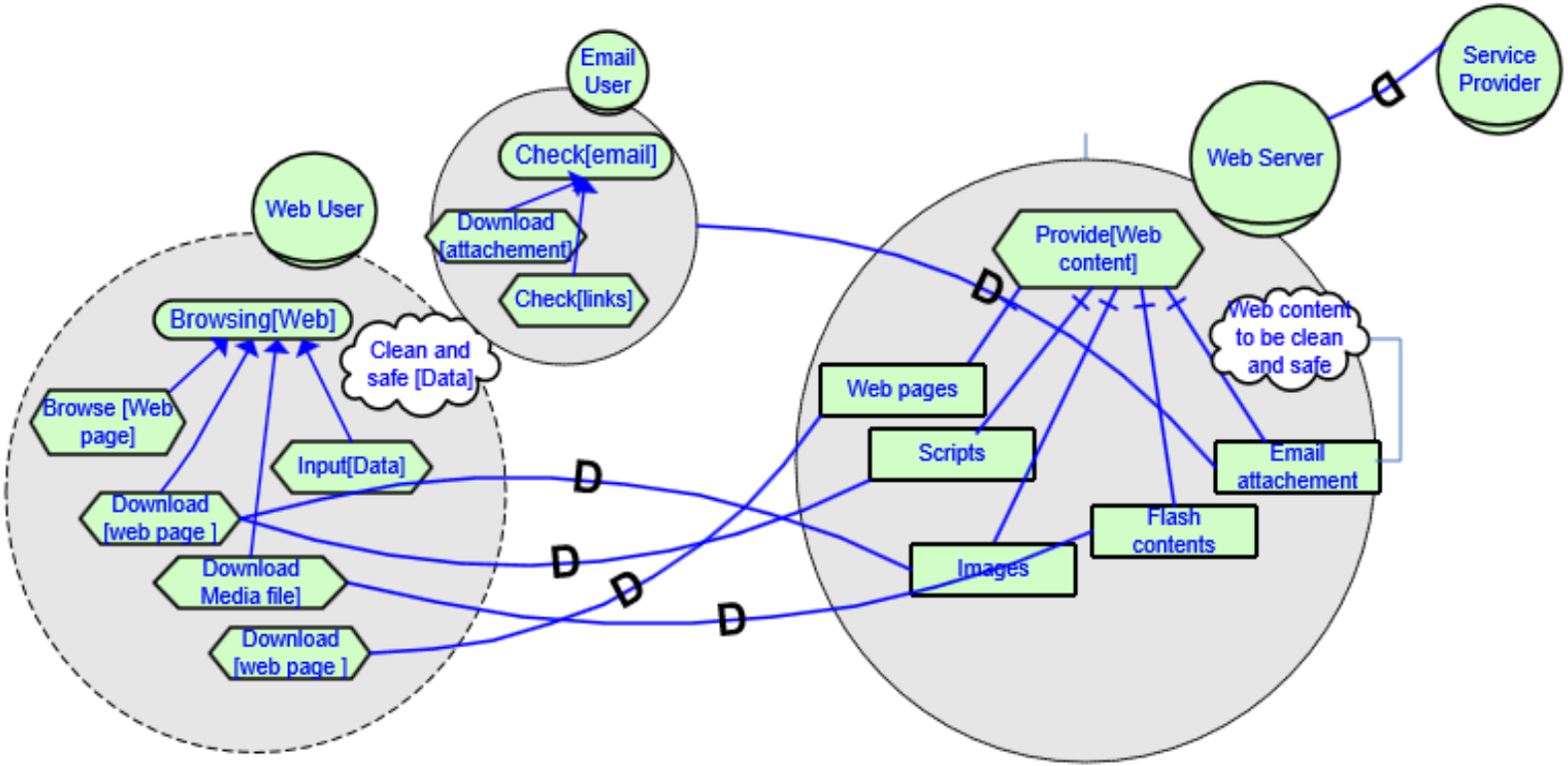
- It mostly be detected when a user cannot be able to access his files.
- A user got different messages which inform him that his data has been encrypted
- There is no perfect mechanism to build a perfect system to detect ransomware.

What are the vulnerabilities In the system?

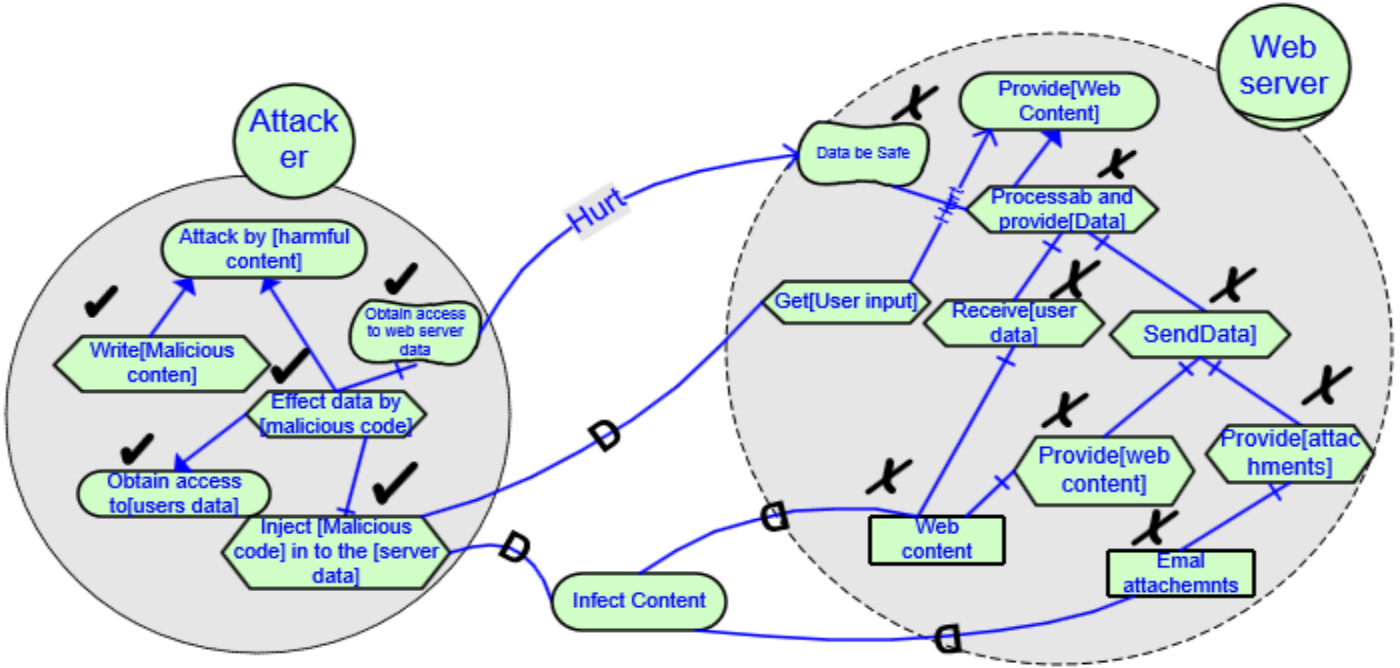
- A system which is already attacked by any malware can be easily targeted. The following are the main vulnerabilities in user system.
- Careless browsing
- Browser weaknesses
- No up to date antivirus
- Download unknown email attachments.
- Pop up enabling

Modeling of Ransomware attack using *i**

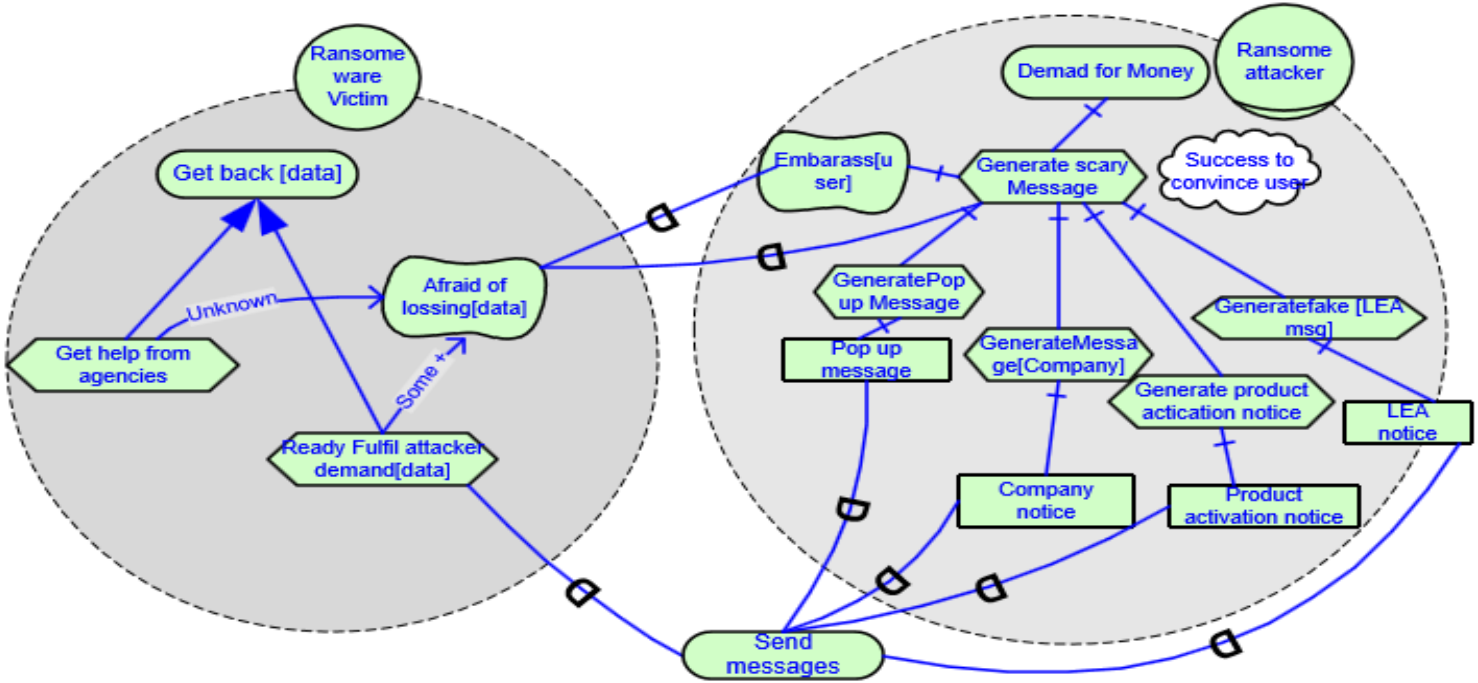
Normal behavior between User and Webserver



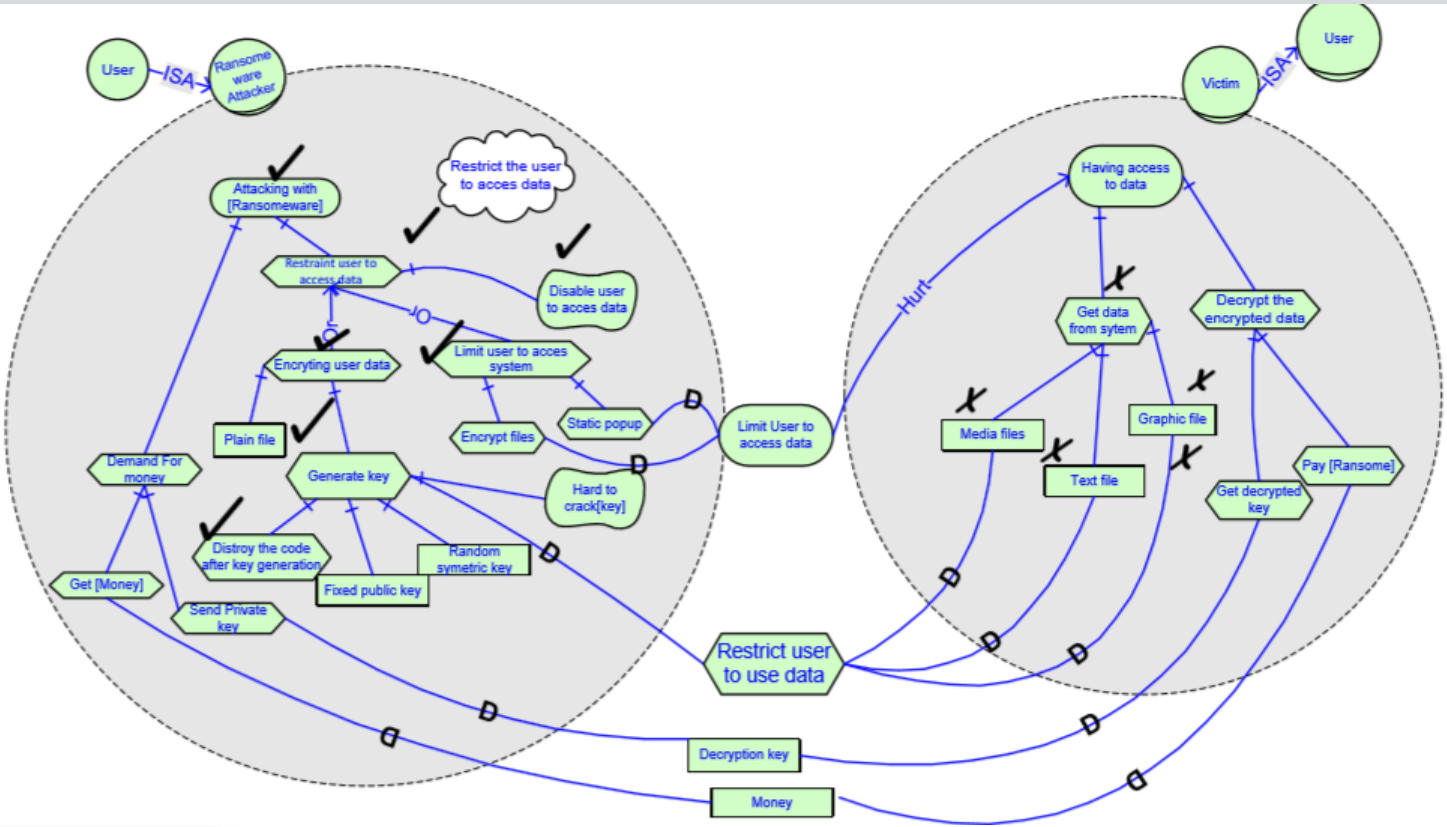
Attacker and Webserver behavior

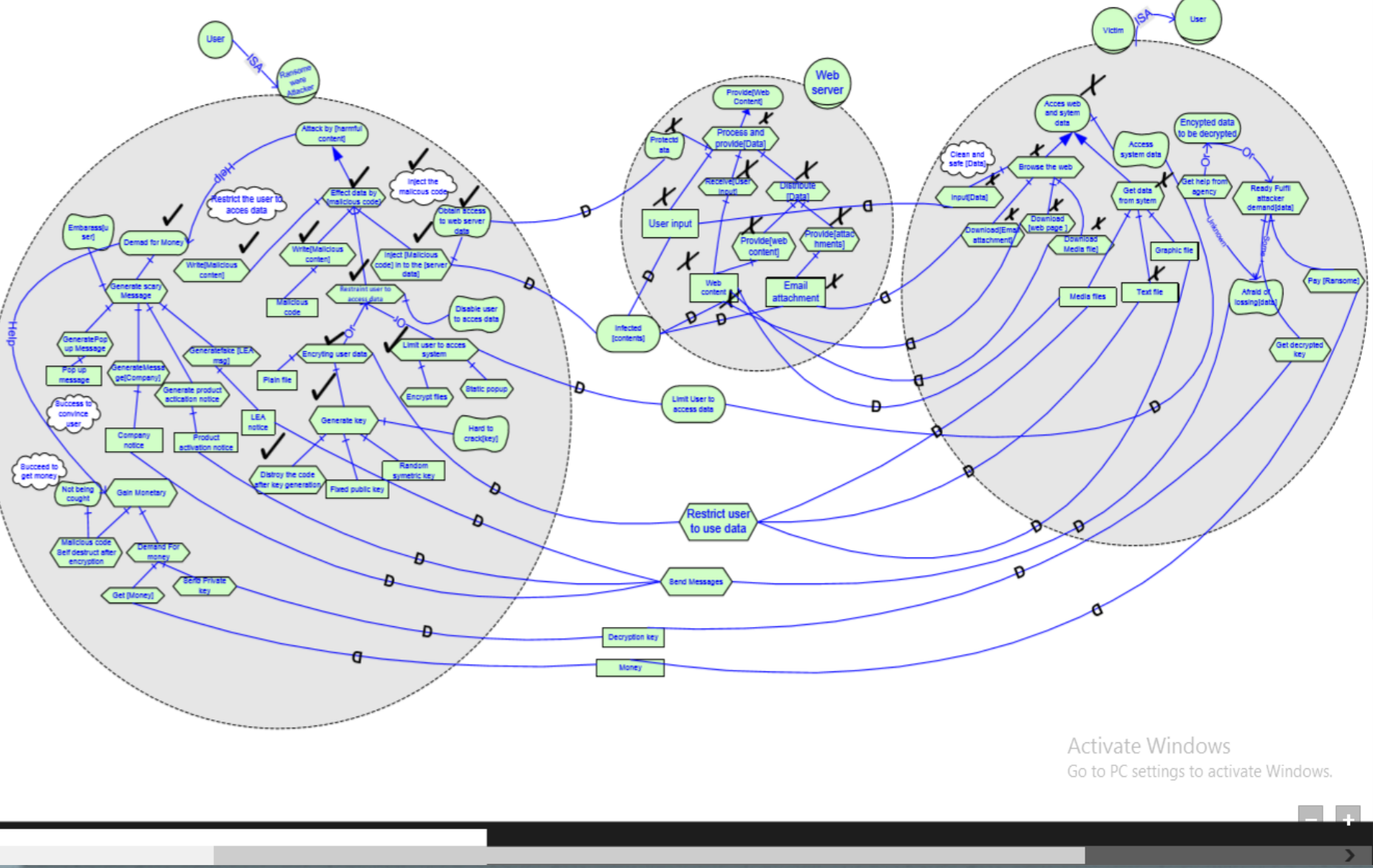


Ransom Demand by attacker

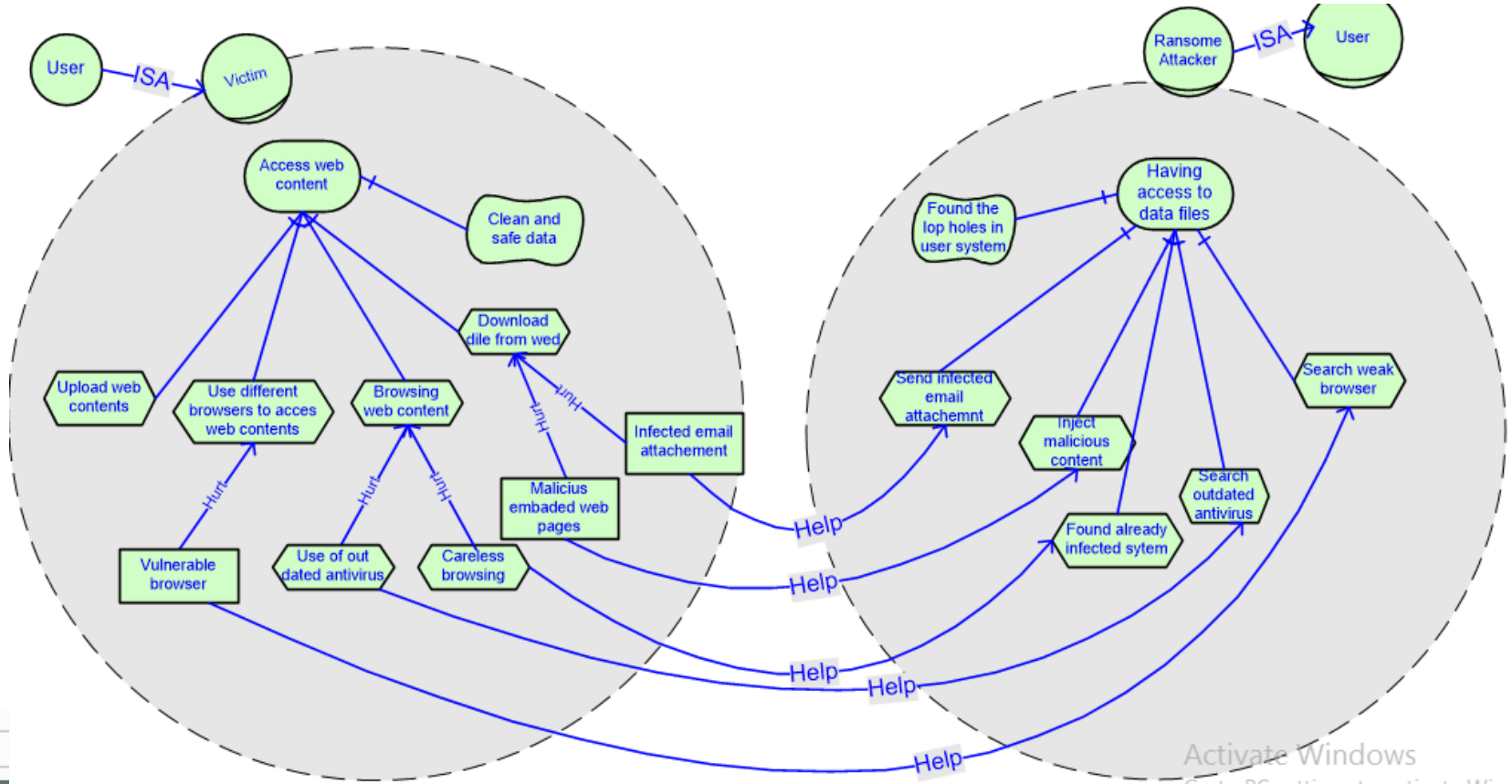


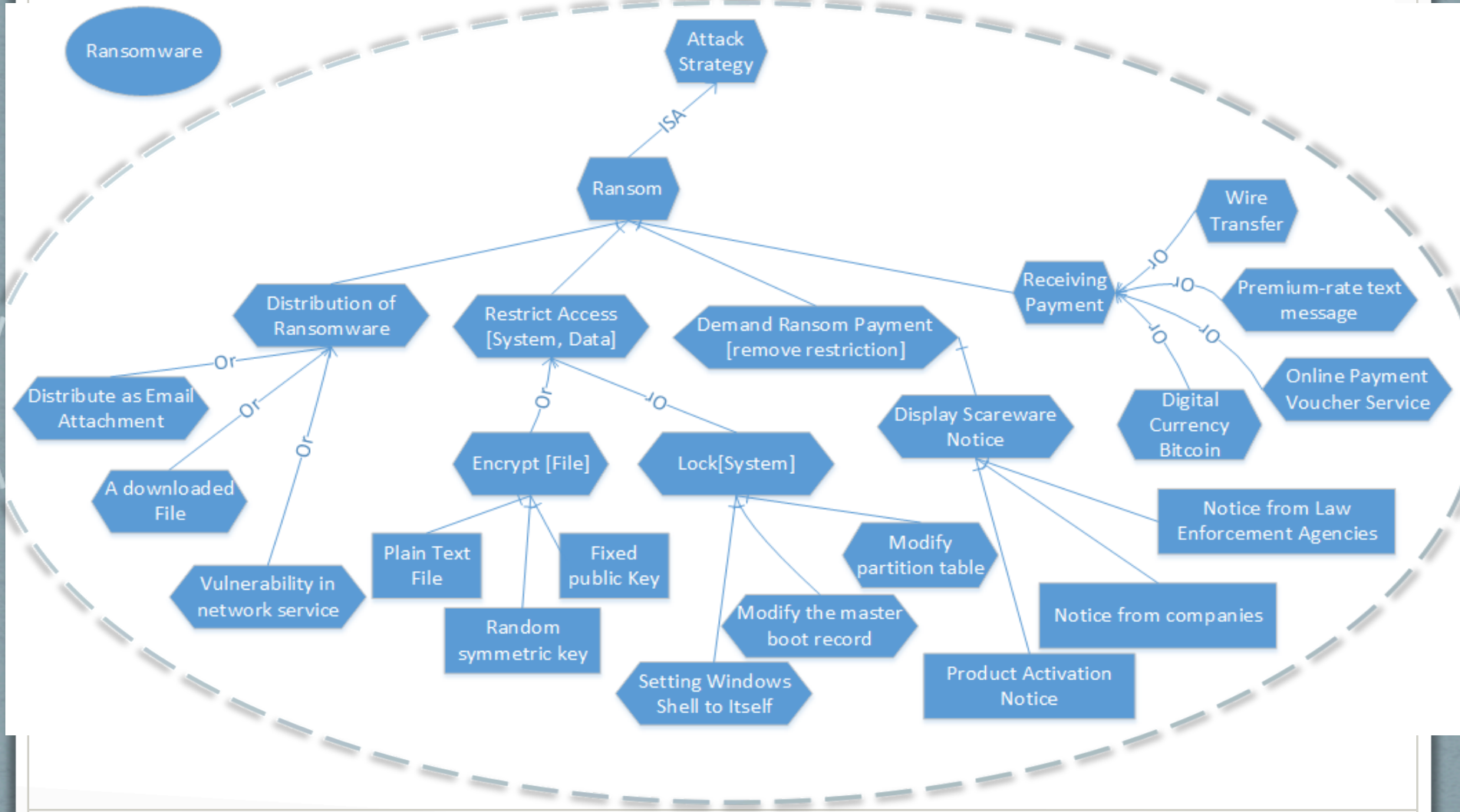
Attacker and victim behavior



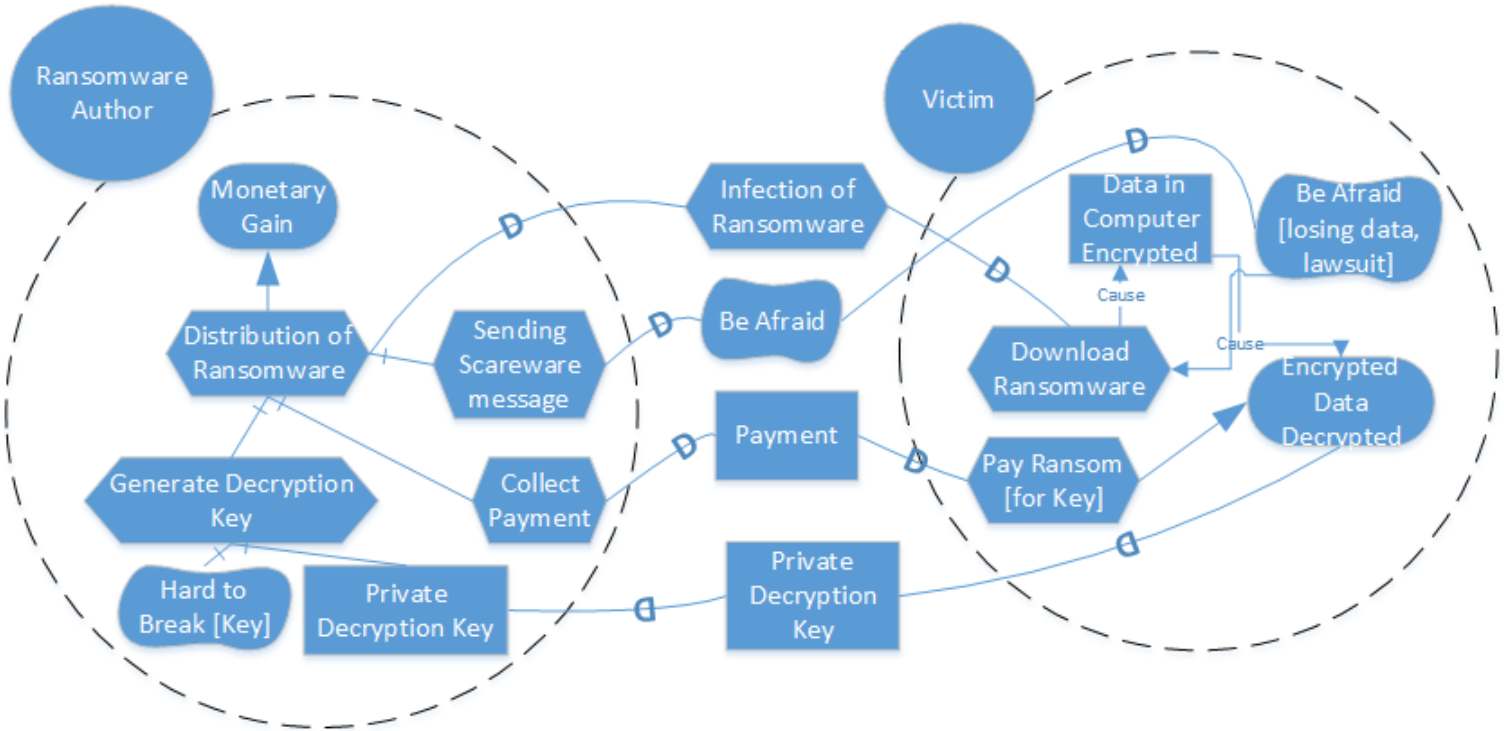

User
ISA
Ransomware attacker
Attack by [harmful content]
Help
Restrict the user to acces data
Effect data by [malicious code]
Inject the malicous code
Obtain access to web server data
Embarrass[user]
Demad for Money
Write[Malicious content]
Write[Malicious content]
Malicious code
Inject [Malicious code] in to the [server data]
Restraint user to access data
Disable user to acces data
Generate scary Message
GeneratePop up Message
Pop up message
GenerateMessage[Company]
Generate product activation notice
Generateface [LEA msg]
Success to convince user
Company notice
Product activation notice
LEA notice
Plain file
Encryting user data
Limit user to acces system
Encrypt files
Static popup
Generate key
Hard to crack[key]
Distroy the code after key generation
Fixed public key
Random symetric key
Succeed to get money
Not being caught
Gain Monetary
Malicious code Self destruct after encryption
Demand For money
Get [Money]
Send Private key
Web server
Provide[Web Content]
Protectdata
Process and provide[Data]
Receive[User input]
Distribute [Data]
User input
Provide[web content]
Provide[attachments]
Web content
Email attachment
Infected [contents]
Victim
ISA
User
Acces web and sytem data
Encypted data to be decrypted
Clean and safe [Data]
Browse the web
Access system data
Input[Data]
Get data from sytem
Get help from agency
Ready Fulfi attacker demand[data]
Download[Email attachment]
Download [web page]
Download Media file]
Graphic file
Media files
Text file
Afraid of lossing[data]
Pay [Ransome]
Get decrypted key
Limit User to access data
Restrict user to use data
Send Messages
Decryption key
Money
Activate Windows
Go to PC settings to activate Windows.

Vulnerabilities in Victim side help attacker

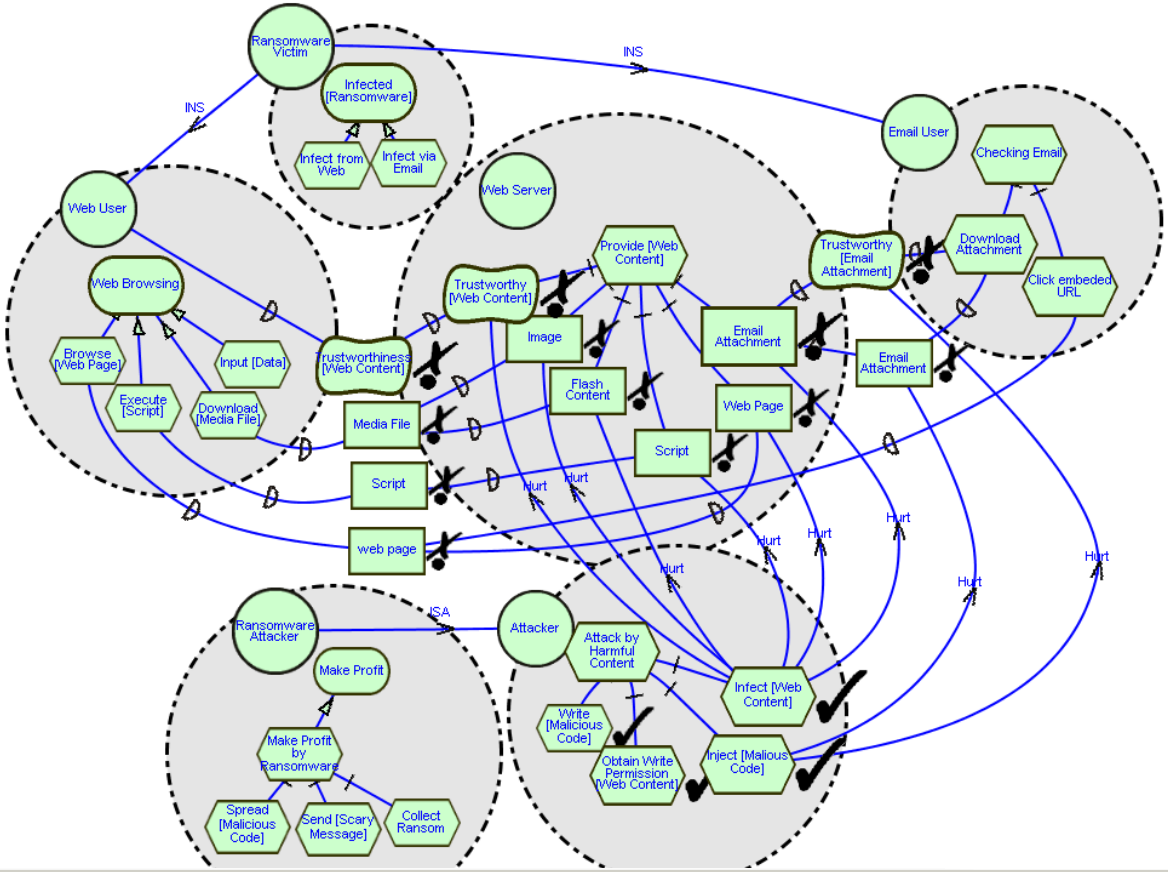



Ransomware
Attack Strategy
ISA
Ransom
Distribution of Ransomware
Restrict Access [System, Data]
Demand Ransom Payment [remove restriction]
Receiving Payment
Wire Transfer
Premium-rate text message
Online Payment Voucher Service
Digital Currency Bitcoin
Or
Distribute as Email Attachment
A downloaded File
Vulnerability in network service
Encrypt [File]
Lock[System]
Plain Text File
Fixed public Key
Random symmetric key
Setting Windows Shell to Itself
Modify the master boot record
Modify partition table
Display Scareware Notice
Notice from Law Enforcement Agencies
Notice from companies
Product Activation Notice

Social Ransomware



Strategic Rationale Modelling of the Ransomware Attack



Discussions

- From the modelling examples above, we conclude that in order to describe the different threats with different causes and impacts, a context model of the attack is needed, which involves social modeling of the attack, especially for intentional attacks.
- In order to limit the negative impact of the incident, we need to identify vulnerabilities in the social infrastructure, and to take actions to prevent threats from happening in future, or to reduce potential loss of a current one, or to recover from a past event, where a social modelling approach will help work out a viable solution from the social dependency perspective.
- It includes: building and evaluating social dependency relationships network at the macro level, and select the best personal/organization for a certain social role at the micro level. This can be turned into a social modeling profile of UML with built-in reasoning abilities.
- It can further implemented as managerial guidelines or information systems functionalities.

References

1. Social Modeling for Requirements Engineering , edited by Eric Yu, Paolo Giorgini, Neil Maiden and John Mylopoulos, MIT press.
2. G. Elahi, E. Yu, Modeling and Analysis of Security Trade-Offs: A Goal Oriented Approach, Data & Knowledge Engineering, Volume 68, Issue 7, July 2009, pp 579-598.
3. C. Liem, Y. Gu, H. Johnson, "A Compiler-Based Infrastructure for Software-Protection", Programming Languages and Analysis for Security (PLAS'08), Tuscon, AZ, June, 2009, pp 33-44.
4. S. Chow, P. Eisen, H. Johnson, P.C. van Oorschot: White-Box Cryptography and an AES Implementation. In: Nyberg, K., Heys, H.M. (eds.) SAC 2002. LNCS, vol. 2595, Springer, Heidelberg (2003) page#s
5. Teng Long, Lin Liu, Yijun Yu, Zhiguo Wan: Assure High Quality Code Using Refactoring and Obfuscation Techniques. FCST 2010: 246-252.
6. Lin Liu, Eric S. K. Yu, John Mylopoulos: Security and Privacy Requirements Analysis within a Social Setting. RE 2003: 151-161.
7. Eric S. K. Yu, Lin Liu: Modelling Trust for System Design Using the i* Strategic Actors Framework. Trust in Cyber-societies 2000: 175-194
8. F. Braber, I. Hogganvik, M. S. Lund, K. Stolen, and F. Vraalsen. Model-based security analysis in seven steps, a guided tour to the CORAS method. BT Technology Journal, 25(1):101--117, 2007.
9. C. Landwehr , A. R. Bull , J. P. Mcdermott, W. , S. Choi, A Taxonomy of Computer Program Security Flaws, 1993.
10. G. Sindre and L. Opdahl. Eliciting security requirements with misuse cases. Requir. Eng., 10(1):34{44, 2005.
11. A. van Lamsweerde. Elaborating security requirements by construction of intentional antimodels. In Proc. of ICSE'04, pages 148--157. IEEE Computer Society, 2004.
12. J. Jurjens. Model-based Security Testing Using UMLsec: A Case Study. Electronic Notes in Theoretical Computer Science, 220(1):93{104, 2008. Proceedings of the Fourth Workshop on Model Based Testing (MBT 2008).
13. Fabio Massacci, John Mylopoulos, Federica Paci, Thein Than Tun, Yijun Yu: An Extended Ontology for Security Requirements. CAiSE Workshops 2011: 622-636
14. Yudistira Asnar, Paolo Giorgini, John Mylopoulos: Goal-driven risk assessment in requirements engineering. Requir. Eng. 16(2): 101-116 (2011)

Thank you ! Questions?