Generating Misuse Cases from Norm Enactments

(Policy-Governed Secure Collaboration, Predictive Security Metrics)

Özgür Kafalı, Munindar P. Singh, and Laurie Williams

Department of Computer Science
North Carolina State University
{rkafali,singh,laurie.williams}@ncsu.edu

Science of Security Seminar
March 23, 2016
Motivation

Problem

- Data breaches pose a great threat to software systems
- Patients suffer from disclosure of their medical records (EHR)
  - Over 350,000 records disclosed from photocopier drives in 2010
  - Over 750,000 records stolen in one incident in 2012
- Often caused due to human misuse (not related to software vulnerabilities)
  - Nurses peeking on celebrity records exploiting emergency privileges
  - Healthcare workers failing to log out from public EHR sessions

http://www.healthcareitnews.com

Kafali, Singh, and Williams (NCSU)  Generating Misuse Cases from Norm Enactments  March 23, 2016
How can we incorporate social interactions into software systems?

STS: modern software systems with technical and social elements

Technical layer: access control mechanisms describe how users access system resources

Social layer: users interact with others on the social level, regulated via social norms
Motivation

Goal

- Current security requirements engineering approaches
determine what mechanisms are needed to protect sensitive resources
- fail to characterize how a user is expected to interact with others
Motivation

Goal

- Current security requirements engineering approaches
  - determine what mechanisms are needed to protect sensitive resources
  - fail to characterize how a user is expected to interact with others

- Our goal is
  - to help security requirements engineering effort
  - by systematically identifying misuse cases from social norms
MUC (Misuse Cases)

- Negative use cases
- New relation types: threatens, mitigates

[Sindre and Opdahl, 2000]
Misuse Case Maps (MUCM)

- Integrate within System Architecture Diagrams (SAD)
- Malicious scenarios depicted as exploit paths
- Regular behavior (black) vs attacks (red)
- Unsuccessful (bar) vs successful attacks (lightning)

[Karpati et al., 2010]
## Limitations

- MUCM provides intuitive visualization to understand intrusions [Karpati et al., 2015]
- However, misuse often arises from interactions among multiple users
- MUCM
  - supports single actor scenarios (no interactions among individual actors)
  - has no computational model for misuse (only informal representation)
  - does not have a rich enough representation for digital forensics (no explicit time)
Social Norms

- **NANE**: a formal framework for identifying malicious activity from Norm Enactments
- Norms provide a natural means to represent requirements
- Directed relation that
  - supports multiple actors
  - provides accountability and sanctioning
- Formalization of norms enables
  - building computational models (first-order logic representation)
  - defining formal relations among norms such as conflicts

---

NANE is Turkish slang for shenanigans
“In most cases, parents are the personal representatives for their minor children. Therefore, in most cases, parents can exercise individual rights, such as access to the medical record, on behalf of their minor children.”

\[A(PARENT, HOSPITAL, representative(PARENT, MINOR), access\_EHR(PARENT, MINOR))\]

[HIPAA, 2003]
“A covered entity must disclose protected health information to HHS when it is undertaking a compliance investigation.”

\[ C(\text{COVERED ENTITY, HHS, investigation(HHS), disclose PHI(COVERED ENTITY, HHS)}) \]
“A covered entity may not disclose protected health information, except the individual who is the subject of the information authorizes in writing.”

\[
P(\text{COVERED ENTITY}, \text{HOSPITAL}, \\
\text{consent}(\text{COVERED ENTITY}, \text{PATIENT}), \\
\text{disclose}_{-}\text{PHI}(\text{COVERED ENTITY}, \_))
\]

[HIPAA, 2003]
Norm Enactments

\[ P(\text{PHYSICIAN}, \text{HOSPITAL}, \neg \text{consent(\text{PHYSICIAN}, \text{PATIENT})} \land \neg \text{emergency, access\_EHR(\text{PHYSICIAN}, \text{PATIENT})}) \]
Norm Enactments

\[ P(\text{PHYSICIAN, HOSPITAL,} \quad 
eg \text{consent(\text{PHYSICIAN, PATIENT})} \land \neg \text{emergency,} \quad \text{access\_EHR(\text{PHYSICIAN, PATIENT})}) \]
Norm Enactments

\[ P(\text{PHYSICIAN, HOSPITAL,} \neg \text{consent(\text{PHYSICIAN, PATIENT}) \land \neg \text{emergency, access}_EHR(\text{PHYSICIAN, PATIENT})} ) \]

\[ \text{access}_EHR(\text{PHYSICIAN, PATIENT}) \]

\[ S_2 \]

Kafalı, Singh, and Williams (NCSU)

Generating Misuse Cases from Norm Enactments
Norm Enactments

\[ P(\text{PHYSICIAN}, \text{HOSPITAL}, \neg \text{consent(\text{PHYSICIAN}, \text{PATIENT})} \land \neg \text{emergency}, \text{access\_EHR(\text{PHYSICIAN}, \text{PATIENT})}) \]

Kafalı, Singh, and Williams (NCSU)
\[ P(\text{PHYSICIAN, HOSPITAL}, \neg \text{consent(\text{PHYSICIAN, PATIENT})} \land \neg \text{emergency, access}\_\text{EHR(\text{PHYSICIAN, PATIENT})}) \]
Norm Enactments

\[ P(\text{PHYSICIAN, HOSPITAL}, \neg \text{consent(\text{PHYSICIAN, PATIENT})} \land \neg \text{emergency}, \text{access\_EHR(\text{PHYSICIAN, PATIENT})}) \]
Refinement

\[ P(\text{PHYSICIAN, HOSPITAL, } \neg\text{consent(}\text{PHYSICIAN, PATIENT}) \land \neg\text{emergency, access}_EHR(\text{PHYSICIAN, PATIENT})) \]
Refinement

\[ P(\text{PHYSICIAN, HOSPITAL,} \neg \text{consent(\text{PHYSICIAN, PATIENT}) \land } \neg \text{emergency, access\_EHR(\text{PHYSICIAN, PATIENT}})) \]

\[ \text{“EHR is usually accessed during a patient visit.”} \]

\[ P(\text{PHYSICIAN, HOSPITAL,} \neg \text{consent(\text{PHYSICIAN, PATIENT}) \lor } \neg \text{visit(PATIENT)} \land } \neg \text{emergency, access\_EHR(\text{PHYSICIAN, PATIENT}})) \]
Enactments after Refinement

visit(PHYSICIAN, PATIENT) → consent(PHYSICIAN, PATIENT) → access_EHR(PHYSICIAN, PATIENT) → S₅

consent(PHYSICIAN, PATIENT) → visit(PHYSICIAN, PATIENT) → access_EHR(PHYSICIAN, PATIENT) → S₆

Kafalı, Singh, and Williams (NCSU)  Generating Misuse Cases from Norm Enactments  March 23, 2016  14 / 19
Enactments after Refinement

visit( PHYSICIAN, PATIENT )

access_EHR( PHYSICIAN, PATIENT )

S1

consent( PHYSICIAN, PATIENT )

access_EHR( PHYSICIAN, PATIENT )

S5 ✓

S6 ✓

access_EHR( PHYSICIAN, NON_PATIENT )

S3 x

consent( PHYSICIAN, PATIENT )

access_EHR( PHYSICIAN, PATIENT )

visit( PHYSICIAN, PATIENT )
Enactments after Refinement

- visit(PHYSICIAN, PATIENT)
- consent(PHYSICIAN, PATIENT)
- access_EHR(PHYSICIAN, PATIENT)
- access_EHR(PHYSICIAN, NON_PATIENT)

States:
- S1
- S2
- S3
- S5
- S6

Valid enactments:
- S5
- S6
Temporal Reasoning for Digital Forensics

% Monday
happens(login(drBob), 8).
happens(access_EHR(drBob, john), 9).
happens(logout(drBob), 10).
happens(give_consent(drBob, john), 16).
happens(give_consent(drBob, kate), 18).
% Tuesday
happens(login(drBob), 32).
happens(access_EHR(drBob, john), 33).
happens(visit(drBob, john), 34).
happens(logout(drBob), 35).
% Wednesday
happens(login(drBob), 56).
happens(access_EHR(drBob, kate), 60).
happens(logout(drBob), 64).

misuse(access_EHR(drBob, john), 9) due to no consent
misuse(access_EHR(drBob,kate), 60) due to no visit
misuse(logout(drBob), 64) due to no logout
Temporal Reasoning for Digital Forensics

% Monday
happens(login(drBob), 8).
\texttt{happens(access\_EHR(drBob, john), 9)}.
\texttt{happens(logout(drBob), 10)}.
\texttt{happens(give\_consent(drBob, john), 16)}.
\texttt{happens(give\_consent(drBob, kate), 18)}.
% Tuesday
\texttt{happens(login(drBob), 32)}.
\texttt{happens(access\_EHR(drBob, john), 33)}.
\texttt{happens(visit(drBob, john), 34)}.
\texttt{happens(logout(drBob), 35)}.
% Wednesday
\texttt{happens(login(drBob), 56)}.
\texttt{happens(access\_EHR(drBob, kate), 60)}.
\texttt{happens(logout(drBob), 64)}.

\texttt{misuse(access\_EHR(drBob, john), 9)} due to no consent
\texttt{misuse(access\_EHR(drBob, kate), 60)} due to no visit
\texttt{misuse(logout(drBob), 64)} due to no logout
Temporal Reasoning for Digital Forensics

% Monday
happens(login(drBob), 8).
happens(access_EHR(drBob, john), 9).
happens(logout(drBob), 10).
happens(give_consent(drBob, john), 16).
happens(give_consent(drBob, kate), 18).

% Tuesday
happens(login(drBob), 32).
happens(access_EHR(drBob, john), 33).
happens(visit(drBob, john), 34).
happens(logout(drBob), 35).

% Wednesday
happens(login(drBob), 56).
happens(access_EHR(drBob, kate), 60).
happens(logout(drBob), 64).

misuse(access_EHR(drBob, john), 9) due to no consent
misuse(access_EHR(drBob, kate), 60) due to no visit
misuse(logout(drBob), 64) due to no logout
Temporal Reasoning for Digital Forensics

% Monday
happens(login(drBob), 8).
happens(access_EHR(drBob, john), 9).
happens(logout(drBob), 10).
happens(give_consent(drBob, john), 16).
happens(give_consent(drBob, kate), 18).
% Tuesday
happens(login(drBob), 32).
happens(access_EHR(drBob, john), 33).
happens(visit(drBob, john), 34).
happens(logout(drBob), 35).
% Wednesday
happens(login(drBob), 56).
happens(access_EHR(drBob, kate), 60).
happens(logout(drBob), 64).

misuse(access_EHR(drBob, john), 9) due to no consent
misuse(access_EHR(drBob, kate), 60) due to no visit
misuse(logout(drBob), 64) due to no logout
User Study

- Norm enactments help identify additional misuse cases?
  - Demonstrate superiority over existing methods in some scenarios, particularly for social misuse cases
  - Complementary to existing methods for some other scenarios

- Collect and analyze data
  - iTrust: an open source medical records system
  - Previous work identified malicious user scenarios for iTrust

http://agile.csc.ncsu.edu/iTrust/wiki/doku.php
Perception: “better” understanding of vulnerabilities regarding the social architecture of a system

Coverage: “better” discovery of misuse cases at design-time

Consistency:
- Identify similar scenarios as misuse cases
- Humans often inconsistent in identification tasks

Relation to test case generation: how can we use (social) misuse cases to evaluate a system’s security?
Theoretical Results

- Sound and complete generation of misuse cases
  - with respect to stated norms
  - based on formal logic proof procedures (verification or temporal reasoning)

- Classification of misuse cases
  - with respect to a priority relation among norms (a norm violation is more severe than another)
  - based on normative closure properties
Open Directions

- Identify missing requirements based on refinement of enactments
- Detect conflicting enactments between functional and non-functional requirements
- Automate norm extraction via NLP
- Domain ontology to complement normative reasoning
- Impact on excessive logging (loss of efficiency and privacy)