CISSA

The Right Tool for the Job:
A Case for Common Input Scenarios for Security Assessment

Xinshu Dong[1], Sumeet Jauhar[1], William G. Temple[1], Binbin Chen[1], Zbigniew Kalbarczyk[2], William H. Sanders[2], Nils Ole Tippenhauer[3] and David M. Nicol[2]

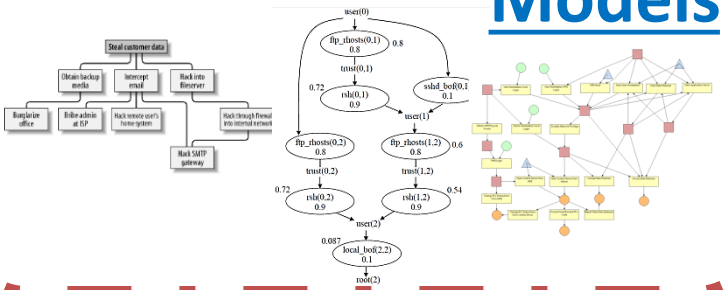
[1] Advanced Digital Sciences Center, Singapore
[2] University of Illinois at Urbana-Champaign, IL
[3] Singapore University of Technology and Design, Singapore

Model-based Security Assessment

- How secure is my/your/their system?

Abstract

Models

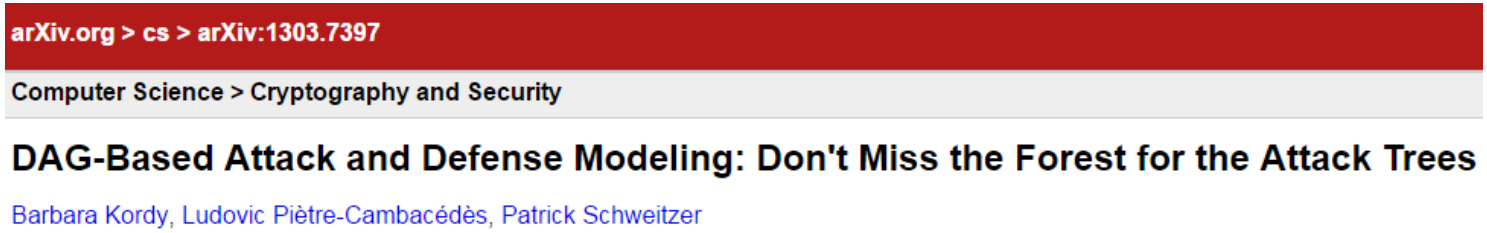


Assess

Reasoning, Metrics,
Decision supports

The Challenges

- We have an impressive range of tools / methodologies


arXiv.org > cs > arXiv:1303.7397

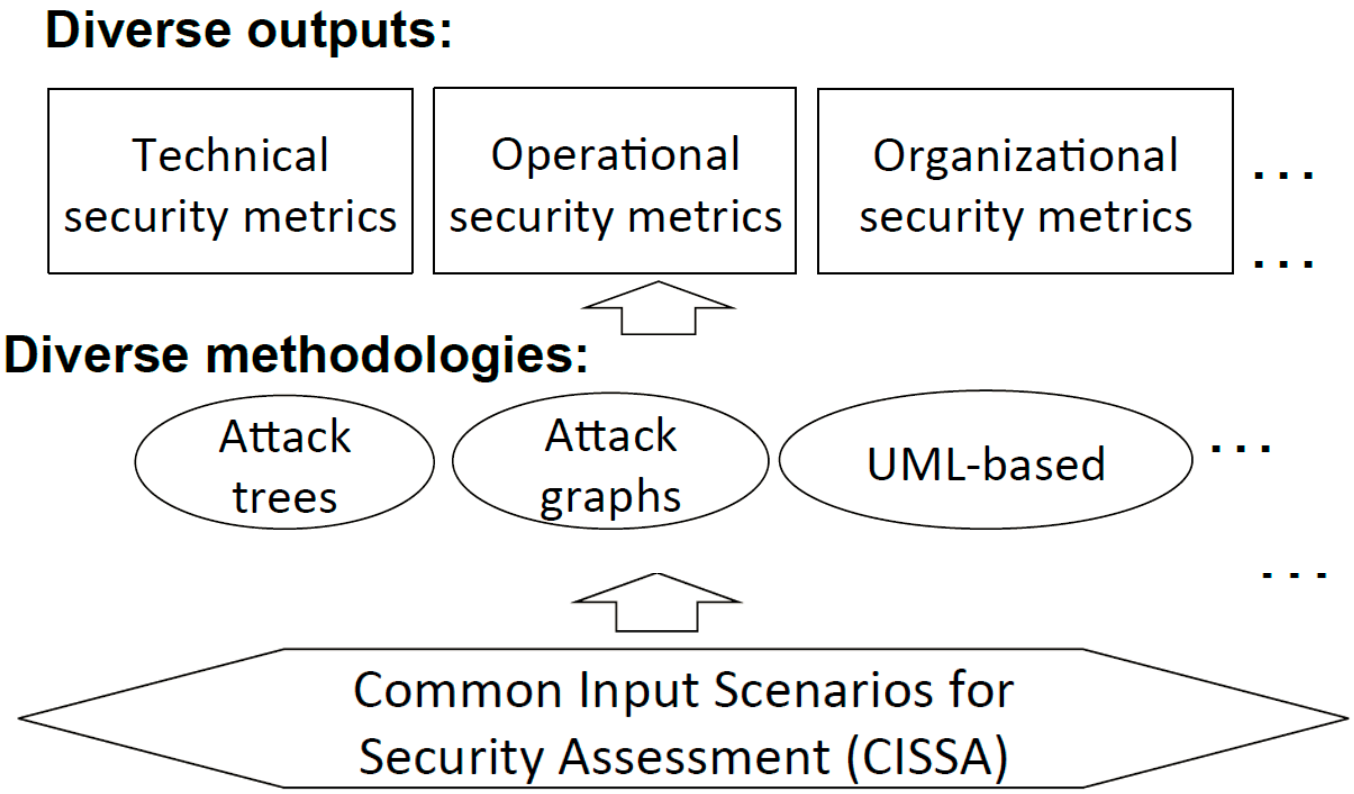
Computer Science > Cryptography and Security

DAG-Based Attack and Defense Modeling: Don't Miss the Forest for the Attack Trees

Barbara Kordy, Ludovic Piètre-Cambacédès, Patrick Schweitzer

- However, there is a lack of conductivity between tool developers & security practitioners
  - Diversity of our methodologies and tool designs makes it challenging to understand their respective strengths, compare or integrate their results

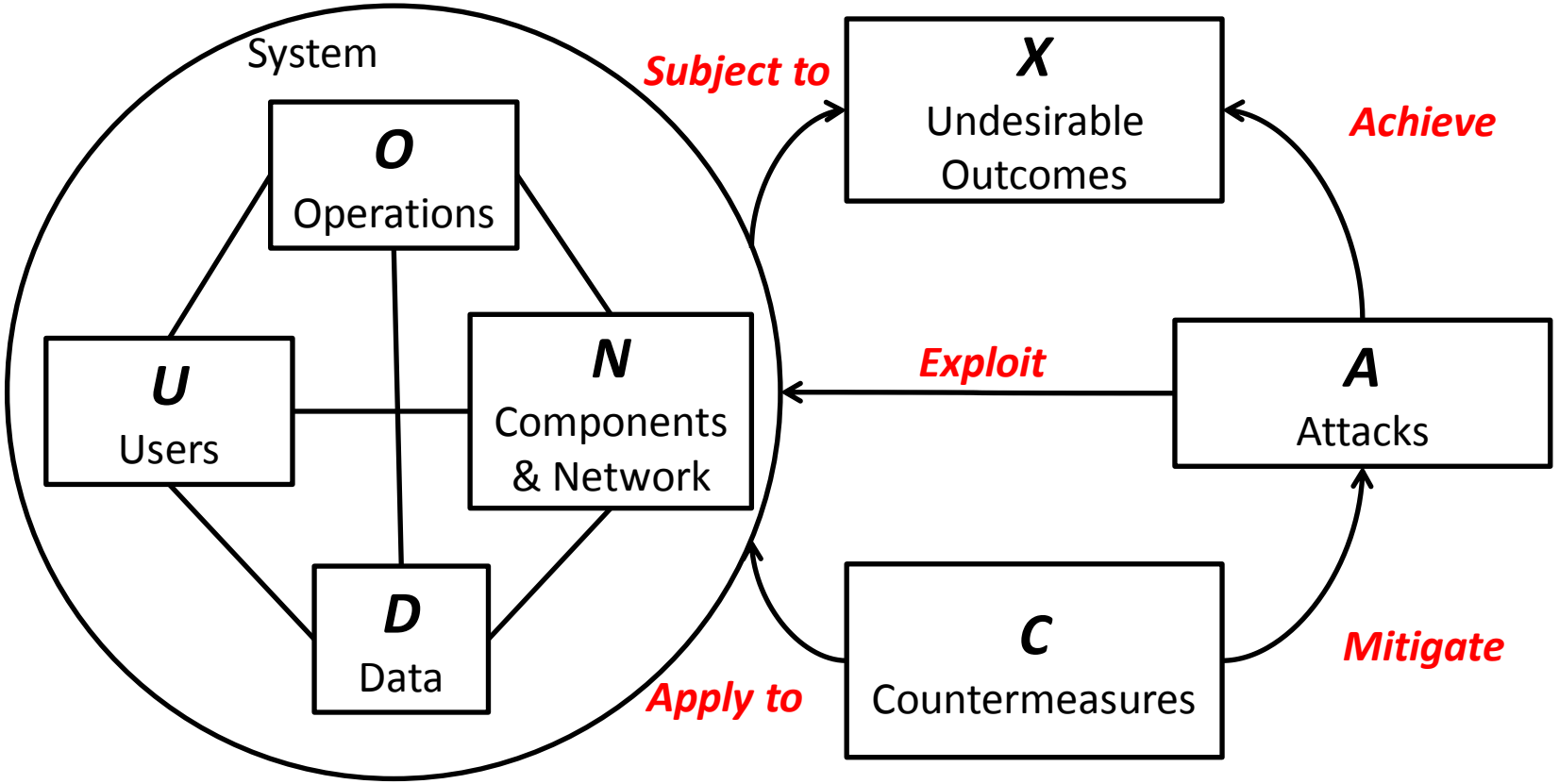
The Envisioned Role of CISSA



Our Contributions

- A framework for specifying *common input scenarios*
  - Organizing **essential info** needed for conducting model-based security assessment
- A feasibility study:
  - Six sample input scenarios based on **real-world cyber incidents**
- Assessment of practical benefits of using CISSA:
  - We **compared** three security assessment tools by applying them to study sample input scenarios

What Constitutes an Input Scenario?

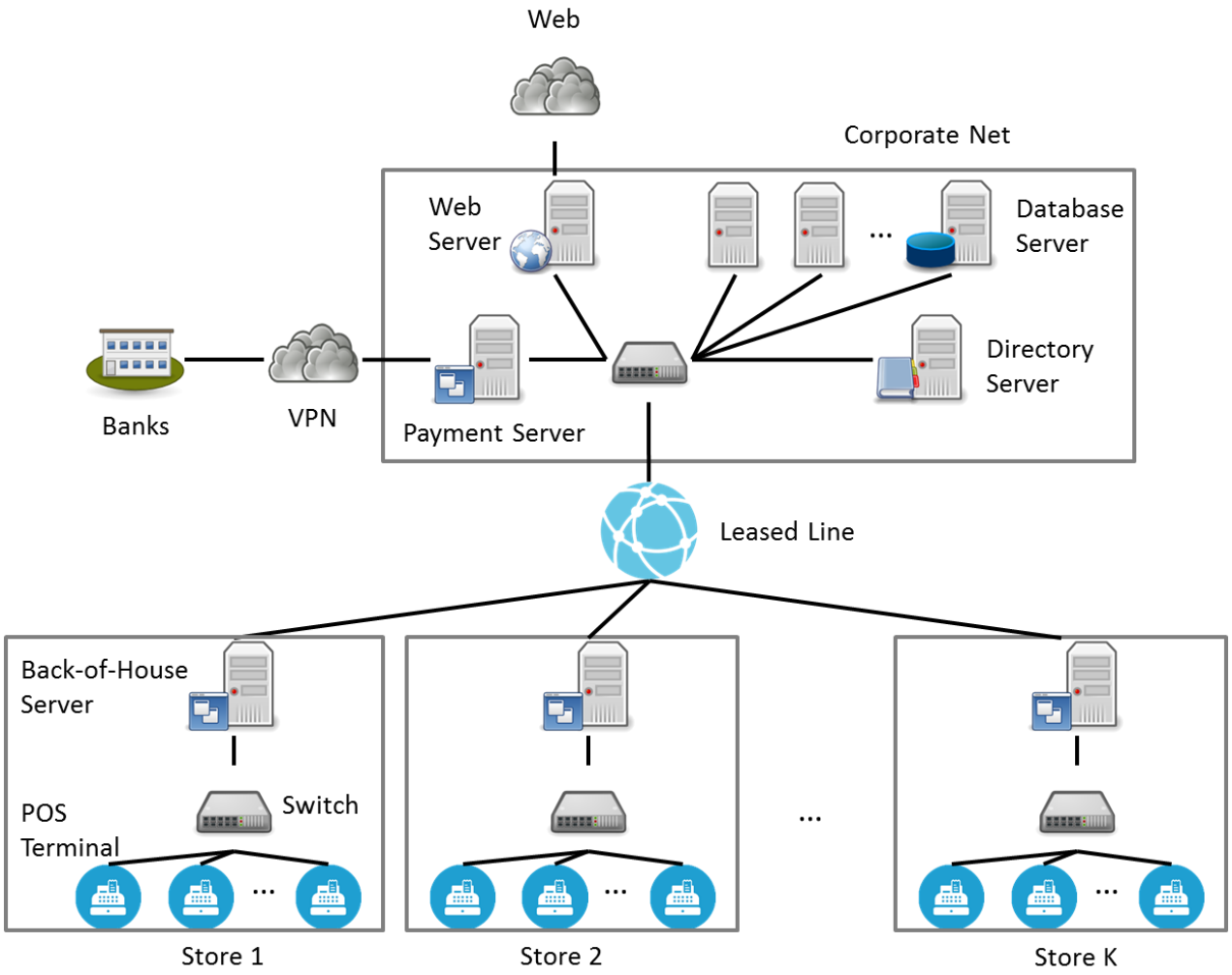


$$< N, D, U, O, X, A, C >$$

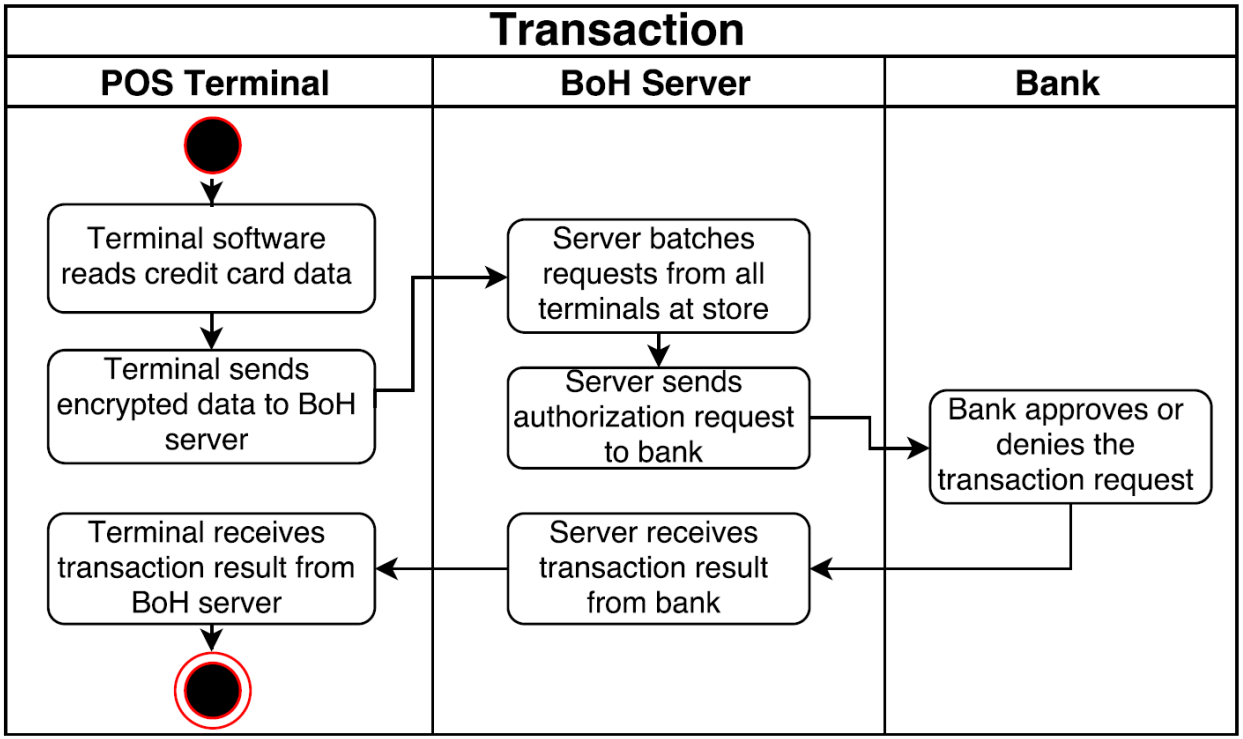
An Example CISSA Case

"Data Breach at Target Corporation, 2013"

(N) Components & Network



(O) Operations



(D) Data

Identifier (ID_D)	**Description** (L_D)	**Mapping** (Map_D)
$D1$	Credit card number	POS terminal, BoH server, Payment server, Bank
$D2$	Customer PII (e.g., name, address)	POS terminal, BoH server, Payment server, Bank, Database Server
$D3$	Admin access token	Servers in corporate network
$D4$	Active Directory listing	Directory server

(U) Users

Identifier (ID_U)	**Description** (L_U)	**Access** (Map_U)
$U1$	Contractor with vendor web portal account	Web server
$U2$	Domain Administrator for corporate network	All devices/links in N
$U3$	Customer in a store	POS terminal

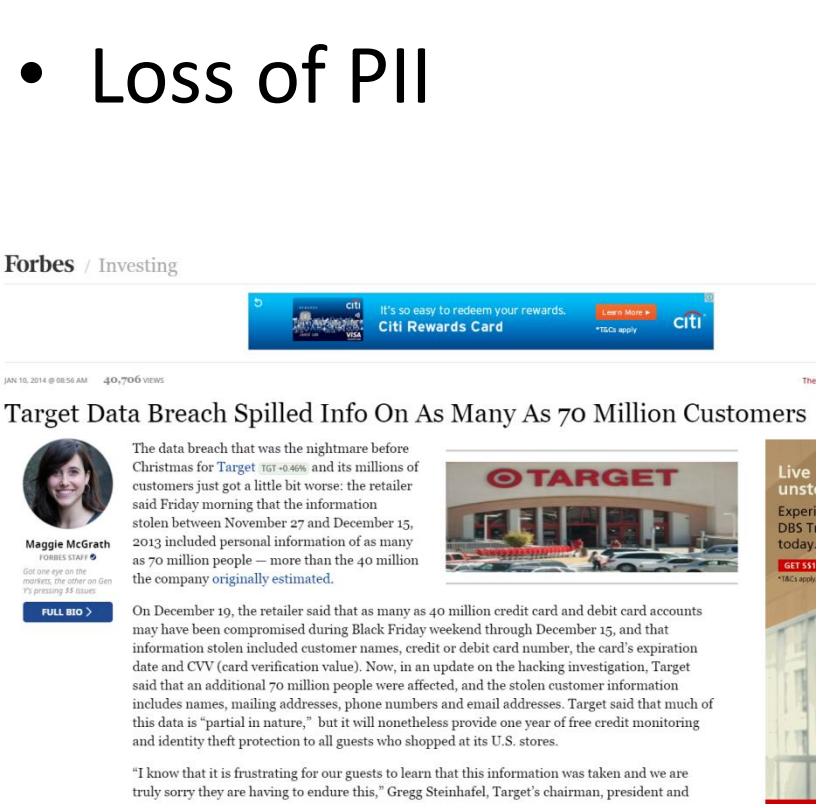
(A) Attack

- Attacker
  - Cyber criminals
- Attack steps

Attack Step (L_σ)	**Pre-Condition** (Pre_σ)	**Post-Condition** ($Post_\sigma$)
1. Steal credentials	<(Vendor's network access), (Server vulnerability exploiting techniques)>	<(Credentials of Target's systems), (), x_1 (Credential leak)>
2. Expl. web server	<(Credentials of Target's systems), (Server vulnerability exploiting techniques)>	<(Privilege to execute OS commands), (), x_2 (Privilege leak)>
3. Steal token	<(Access to Target's servers), (Know-how of collecting NT hashes from memory)>	<(Corporate network admin privilege), (), x_3 (Privilege escalation)>
4. Create account	<(Admin privilege to add new user to Domain), ()>	<(Access to corporate network), (), x_4 (Malicious admin account)>
5. Steal PII	<(Access to corporate network), (Skill to use database server)>	<(Access to customer records), (), x_5 (Unauthorized access)>
6. Install malware	<(Access to POS machines' writable folders), (Malware infection capabilities)>,	<(Access to data on POS), (), x_6 (Malware infection)>
7. Aggregate data	<(Access to FTP servers in corporate network, access to sensitive data), (Basic file transfer techniques)>	<(), (), x_7 (Sensitive data aggregated>
8. Exfiltrate data	<(Access to outward-facing internet connection, access to sensitive data), (Skills to stealthily exfiltrate files)>	<(), (), $X1 \cup X2$ (Data leak)>

(X) Undesirable Outcomes

- Loss of credit card data
- Loss of PII



Forbes / Investing

JAN 10, 2014 @ 08:56 AM 40,706 VIEWS

Target Data Breach Spilled Info On As Many As 70 Million Customers

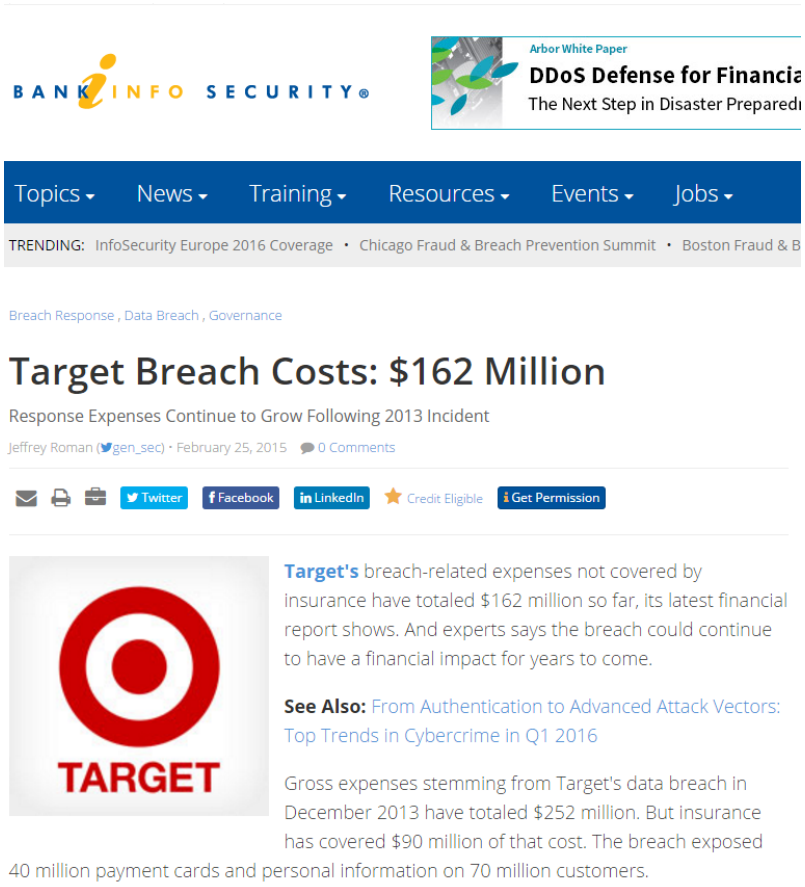
Maggie McGrath
FORBES STAFF

FULL BIO >

The data breach that was the nightmare before Christmas for Target TGT +0.46% and its millions of customers just got a little bit worse: the retailer said Friday morning that the information stolen between November 27 and December 15, 2013 included personal information of as many as 70 million people — more than the 40 million the company originally estimated.

On December 19, the retailer said that as many as 40 million credit card and debit card accounts may have been compromised during Black Friday weekend through December 15, and that information stolen included customer names, credit or debit card number, the card's expiration date and CVV (card verification value). Now, in an update on the hacking investigation, Target said that an additional 70 million people were affected, and the stolen customer information includes names, mailing addresses, phone numbers and email addresses. Target said that much of this data is "partial in nature," but it will nonetheless provide one year of free credit monitoring and identity theft protection to all guests who shopped at its U.S. stores.

"I know that it is frustrating for our guests to learn that this information was taken and we are truly sorry they are having to endure this," Gregg Steinhafel, Target's chairman, president and



BANK INFO SECURITY

Topics News Training Resources Events Jobs

TRENDING: InfoSecurity Europe 2016 Coverage • Chicago Fraud & Breach Prevention Summit • Boston Fraud & B

Breach Response , Data Breach , Governance

Target Breach Costs: $162 Million

Response Expenses Continue to Grow Following 2013 Incident

Jeffrey Roman (gen_sec) • February 25, 2015 0 Comments

Twitter Facebook LinkedIn Credit Eligible Get Permission

TARGET

Target's breach-related expenses not covered by insurance have totaled $162 million so far, its latest financial report shows. And experts says the breach could continue to have a financial impact for years to come.

See Also: From Authentication to Advanced Attack Vectors: Top Trends in Cybercrime in Q1 2016

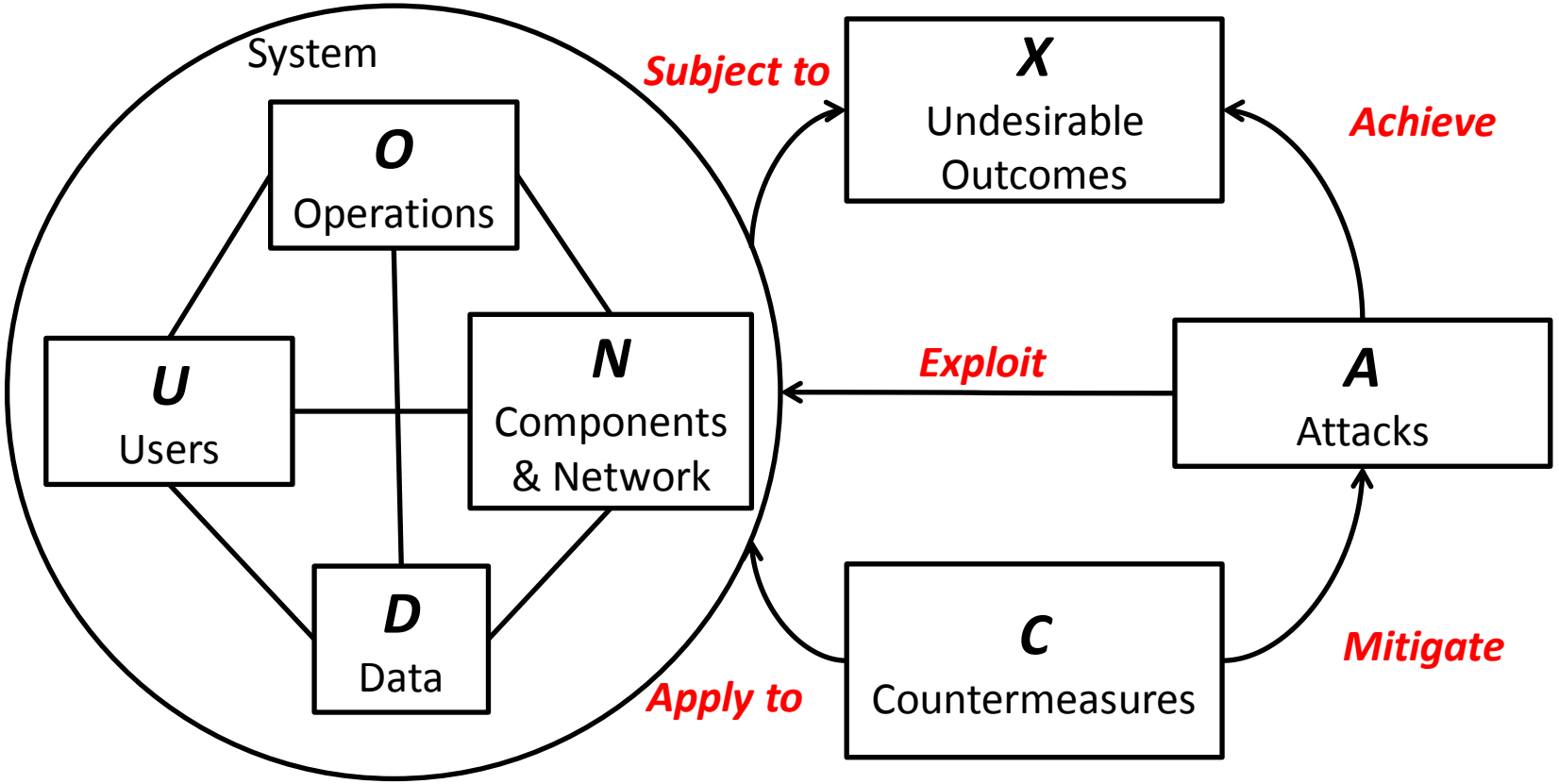
Gross expenses stemming from Target's data breach in December 2013 have totaled $252 million. But insurance has covered $90 million of that cost. The breach exposed 40 million payment cards and personal information on 70 million customers.

(C) Countermeasures

- Perimeter defense mechanisms
  - Firewalls, access control, etc.
- Intrusion detection/prevention
- End-point security
  - Timely patching, updated antivirus, disabled USB port, etc.

- ***How effective are they in thwarting attacks?***
- ***What are the associated costs?***

Putting everything together



$$< N, D, U, O, X, A, C >$$

An Initiative to Build CISSA Repository

- Publicly available at http://www.illinois.adsc.com.sg/cissa/
  - 6 CISSA cases
  - Each case contains XML files for the 7 CISSA elements

CISSA Scenario	Unique Characteristics
Stuxnet	Multi-step, several zero-day exploits, broken "air-gap", command & control
Maroochy	Insider attack, poor auditing and access control policy, sabotage
Dragonfly	Targeted attack, watering hole, multi-step, trojanized software update, command & control
Target	Data breach, multi-step, integrated but insufficient security mechanisms, delayed incident response
SK Communications	Highly targeted attack, data breach, poor security policy, trojanized software update
Syrian Electronic Army	Targeted attack, multi-step, evading detection and defense

Lessons Learned

- The need for iteration
  - We added the **user** input after identifying a gap in a previous ontology related to the modeling of human-centric attack vectors such as phishing
  - We found it hard to decide the level of details to be included in CISSA
    - Real-world systems incidents are complex
    - There may be no “right” level of details

Evaluating Security Assessment Tools using CISSA

CISSA in Use

- We use CISSA to study 3 different security assessment tools

Tool	Category	Features
MulVAL [19]	Attack-graph-based	Integrating network & system vulnerability assessment
CySeMoL [27]	UML-based	Modeling various aspects of information system, with built-in knowledge base for quantitative evaluation
BDMP [23, 22]	Attack-tree-alike, with extra modeling power	Modeling dynamic behaviors by Markov-chain-enhanced attack trees

  - We apply a *best-effort* approach here
  - All three tools need extra information beyond CISSA inputs

The Goal of Our Evaluation

- Does a common ground provided by CISSA shed light on comparing and selecting existing security assessment tools?

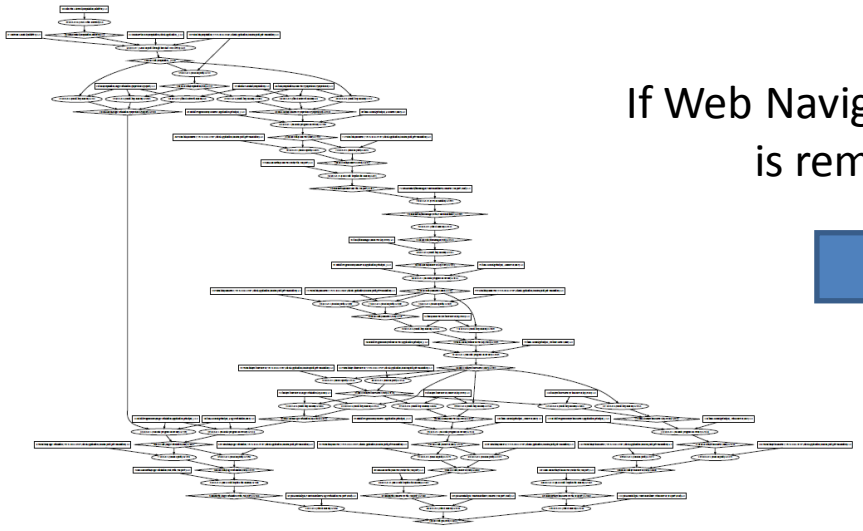
- Does CISSA help reveal aspects where existing assessment tools are doing well and/or can be improved?

Security Aspect/Features in Tool Assessment

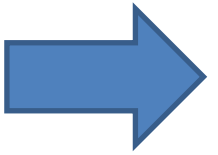
- ***Technical:*** *e.g., how do the network topology and configuration of the assessed system affect its security standing, for a particular scenario?*
- ***Operational:*** *e.g., how much would a better incident response procedure change the system's resilience against the given attack?*
- ***Organizational:*** *e.g., how effective could a better security awareness program be at thwarting an attack in a given environment?*

Experiment I: Technical Aspects (Impact of Network Configuration)

- MulVAL can easily model topology changes



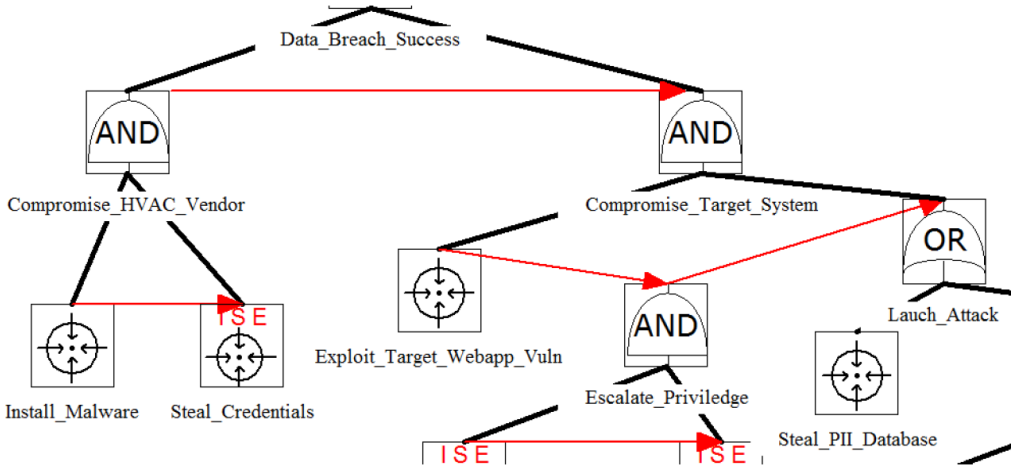
If Web Navigator server is removed



- BDMP: One needs to manually change the model to study the impact of varying network topologies and configuration setup
- CySeMoL: Manual construction in the beginning, but easier to alter and re-run experiments

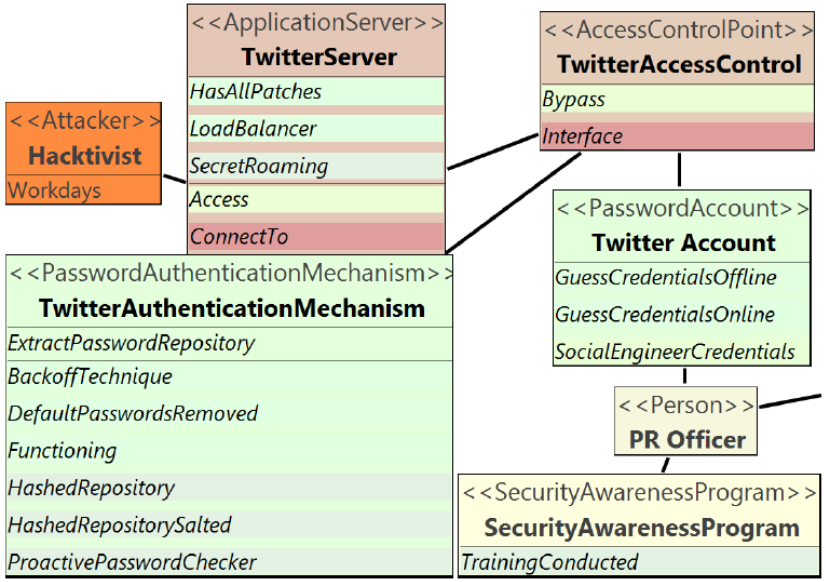
Experiment II ---- Operational Aspects

- Impacts of a better incident response procedure?
  - No explicit built-in notion of time in MulVAL
  - CySeMoL allows users to vary the attack duration parameter, which indirectly models the response
  - BDMP provides direct modeling support of defense



Experiment III ---- Organizational Aspects

- Impact of a better security awareness program?
  - CySeMol has a built-in model for **"SecurityAwarenessProgram"**
  - In general, organizational aspects are less well modeled in existing tools



Observations

- The need to clarify inputs explicitly
  - A tool's input = CISSA + Δ
  - Different Δ leads to different outputs, e.g.,:

Tool	10 Days' Attack	30 Days' Attack	180 Days' Attack
CySeMoL	.38	.43	.45
BDMP	.05	.34	.60

- Integration of different tools
  - Each has its unique strength
- Modeling security beyond technical level
  - We see less support when we move from technical- to operational- to organizational-level modeling

Looking Forward

- Need more CISSA cases
  - Different categories
  - Different attack tactics
  - Different system & network topologies and defenses
- Need more iterations about the basis
  - Hopefully converging on some usable framework
  - Collectively decide what information should be included
  - Come up with benchmarks / metrics for comparing the tools
- Most importantly: Attract people to use them
  - Approach: Devise parsers that convert CISSA to inputs of different tools
  - Goal: More case-driven cross-comparison among different tools

Call for Action:
Sustained community effort is needed