Game-Theoretic Approach to Feedback-Driven Multi-Stage Moving Target Defense

Quanyan Zhu\textsuperscript{1} and Tamer Ba\c{s}ar\textsuperscript{2}

\textsuperscript{1}Department of Electrical Engineering
Princeton University

\textsuperscript{2}Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign

October 3, 2013
Outline

• Motivation
• Science of Security
  – Game-Theoretic Framework
  – Feedback Control System Model
• Examples
• Conclusions
Motivation

• The *static nature* of computing systems facilitates an attacker’s capability of gathering information and executing attacks.

• The network security can be improved by changing the appearance of the system and creating a *moving target*.
  - The availability of services will be *time-varying* under different system configurations, and the system can block dangerous network behaviors if an attacker does not follow the *network dynamics*.
  - An attacker has to spend a significant amount of resources to carefully guide his attacks.
How to shift attack surface?
How to quantify moving target defense?

Our goal: *A Scientific Foundation for Moving Target Defense*
Abstraction
Abstraction
• \( f \) and \( g \) are mixed strategies. Mixed strategies are *randomizing* strategies.
Not Sufficient Yet!

- Does not inform us how to reach the equilibrium.
- There is no feedback in the model.
- Does not consider the cost for randomization.
- Payoffs may not be known.

\[
\begin{array}{c|ccc}
   & a_{1,1} & a_{1,2} & a_{1,3} \\
\hline
   c_{1,1} & 1 & 2 & 0 \\
   c_{1,2} & 0 & 2 & 3 \\
\end{array}
\]

- \(f\) and \(g\) are mixed strategies. Mixed strategies are \textit{randomizing} strategies.
A Feedback System Model

- Shift Attack Surface
- Risk Learning
- Update Moving Target Defense

Symbols:
- $\mathcal{C}_{l,t}$
- $f_{l,t+1}$
- $\hat{r}_{l,t}$
- $r_{l,t}$
- $\hat{r}_{l,t}^S$
$$\hat{r}_{l,t+1}^S(c_{l,h}) = \hat{r}_{l,t}^S(c_{l,h}) + \mu_t^S \mathbb{1}_{\{c_{l,t}=c_{l,h}\}}(r_{l,t} - \hat{r}_{l,t}^S(c_{l,h})),$$

$$\hat{r}_{l,t+1}^A(a_{l,h}) = \hat{r}_{l,t}^A(a_{l,h}) + \mu_t^A \mathbb{1}_{\{a_{l,t}=a_{l,h}\}}(r_{l,t} - \hat{r}_{l,t}^A(a_{l,h})).$$
(SP) \[ \sup_{f_{l,t+1} \in \mathcal{F}_l} \langle f_{l,t+1}, -\hat{r}_{l,t}^S \rangle - \epsilon_{l,t}^S \sum_{h=1}^{m_l} f_{l,h,t+1} \ln \left( \frac{f_{l,h,t+1}}{f_{l,h,t}} \right) . \]

Average risk to be minimized

Relative entropy: Distance between two distributions

Cost on changing the strategy (usability)

\[ f_{l,h,t+1} = \frac{f_{l,h,t+1} e^{-\hat{r}_{l,t}(c_l,h)}}{\epsilon_{l,t}^S} \]

\[ \sum_{h'=1}^{m_l} f_{l,h',t} e^{-\hat{r}_{l,t}(c_l,h')} \epsilon_{l,t}^S \]
A Feedback System Model

System

Shift Attack Surface

Update Moving Target Defense

Risk Learning

$C_{l,t}$

$f_{l,t+1}$

$r_{l,t}$

$\hat{r}_{l,t}^S$
Mathematical Analysis of the Feedback System

\[ \hat{r}_{l,t+1}(c_l,h) = \hat{r}_{l,t}(c_l,h) + \mu_t^S \mathbb{1}_{\{c_l,t = c_l,h\}}(r_{l,t} - \hat{r}_{l,t}^S(c_l,h)) \]

\[ f_{l,h,t+1} = (1 - \lambda_{l,t}^S)f_{l,h,t} + \lambda_{l,t}^S \left( \frac{-\hat{r}_{l,t}(c_l,h)}{\epsilon_{l,t}^S} \right) \]

- Use stochastic approximation to show the convergence to an ordinary differential equation (ODE).
- Use ODE to show the convergence of the coupled dynamics to the equilibrium
Strategy of the defender:
Choosing between two configurations $c_{1,1}$ and $c_{1,2}$

Strategy of the attacker:
Choosing between three attacks $a_{1,1}$, $a_{1,2}$, $a_{1,3}$
Payoff of the defender: Choosing between two configurations $c_{1,1}$ and $c_{1,2}$

Payoff of the defender: Choosing between three attacks $a_{1,1}$, $a_{1,2}$, $a_{1,3}$
Real-Time Estimated Risk of Using Configurations $c_{1,1}$ and $c_{1,2}$

- From $t = 99$ to $t = 115$, the system sees an unusual peak of risk under $c_{1,2}$. This exogenous input models unexpected malicious events or alerts due to the potential risk imposed by $v_{1,1}$.
• The higher risk imposed by $c_{1,2}$ increases the probability of using the alternative strategy $c_{1,1}$.
Real-Time Strategy Update for Non-Rational Attacker

- Larger $\epsilon$: More costly for the system to change its attack surface regularly.
- Smaller $\epsilon$: More agile in response to the attacker
System Vulnerability Metric: \[ \psi_l(f_l, g_l) := d_{KL}(\eta_l \| g_l) = \sum_{h=1}^{n_l} \eta_{l,h} \ln \left( \frac{\eta_{l,h}}{g_{l,h}} \right). \]

Measures the alignment between attack and defense strategies.

- Higher \( \Psi \) \( \rightarrow \) Worse Alignment \( \rightarrow \) Less Vulnerable
- Moving target defense yields less vulnerable defense than static randomization.
Multi-Stage Attack Graph of Stuxnet

Creator

Contractor/Tradeshow

Employee

Target Industrial Process

Industrial Process

S7-417 Safety PLCs

I/O Modification

Engrg. Station

S7-417 Safety PLCs

Logic Modification

I/O Modification

Control System Network

Process Control Network

Perimeter Network

Historian Workstn

CAS Server

Web Nav. Server

Engrg. Station

S7-417 Safety PLCs

Target Industrial Process

WinCC DB Exploitation

Vulnerability Exploitation

Network Share S7 Project Files

Logic Modification

I/O Modification

Credential Harvesting

Employee Workstn.

Vulnerability Exploitation

Shared Network

Enterprise Control Network

Initial Asset

External
Extension of the Framework to Multi-Stage Attack Graph of Stuxnet

- Moving target defense is used at each stage.
- Payoff includes current and look-ahead costs.
- Costs are measured by satisfiability of security policies.
Conclusions and Future Work

• Moving target defense is an alternative solution to the current expensive and imperfect detection of an intelligent attacker.

• We have developed a game-theoretic framework and a feedback mechanism for guiding the quantitative design of moving target defense as a tradeoff between security and usability.

• Towards science of security.

• This work could be further extended to a stochastic game framework where transition probabilities between games capture strategy interdependencies across the layers.