Learning security strategies

Dusko Pavlovic
University of Hawaii

C3E
June 2015

Outline

Problem: Strategic bias

Background: Attacker models

Approach: Learning strategies

Summary

Outline

Problem: Strategic bias

Background: Attacker models

Approach: Learning strategies

Summary

Cyber problems

cyber war

cyber bullying

cyber crime

What do they have in common?

Cyber problems

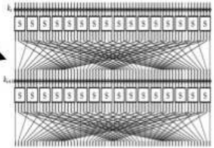
cyber war

cyber bullying

cyber crime

It is easier to attack then to defend

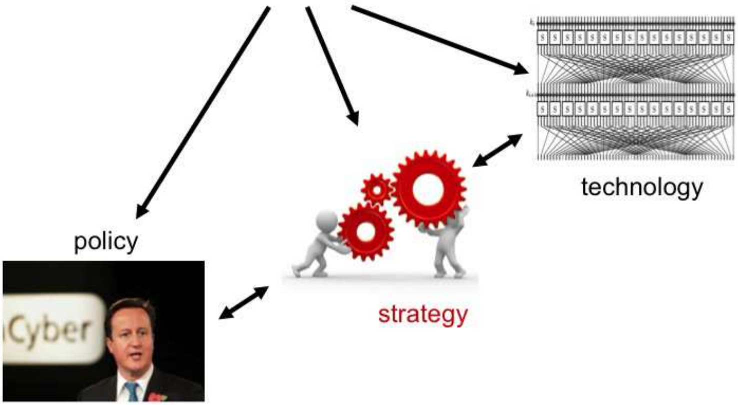
Cyber solutions



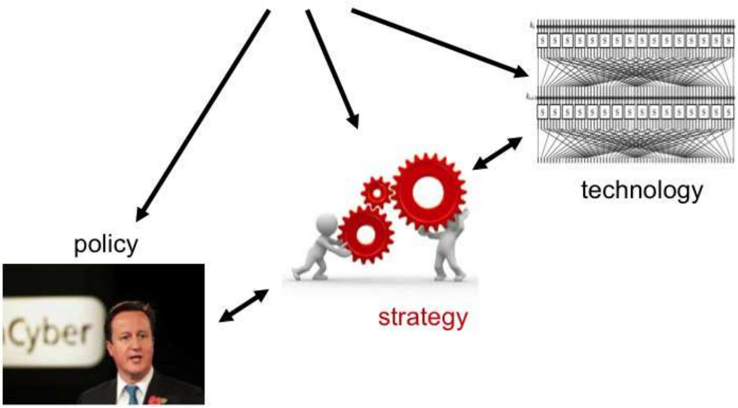
technology

policy

Cyber solutions

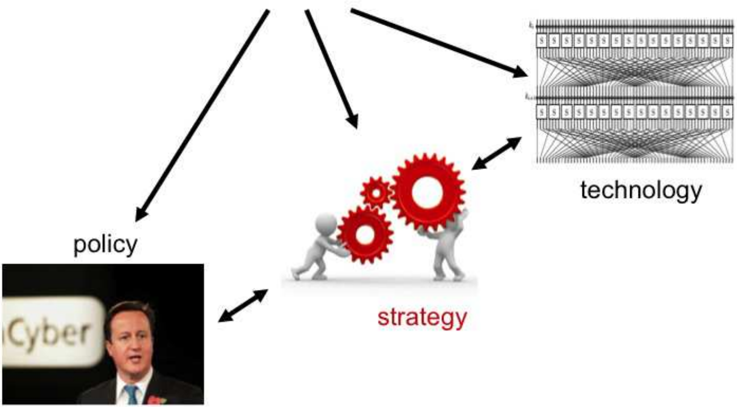


Cyber solutions



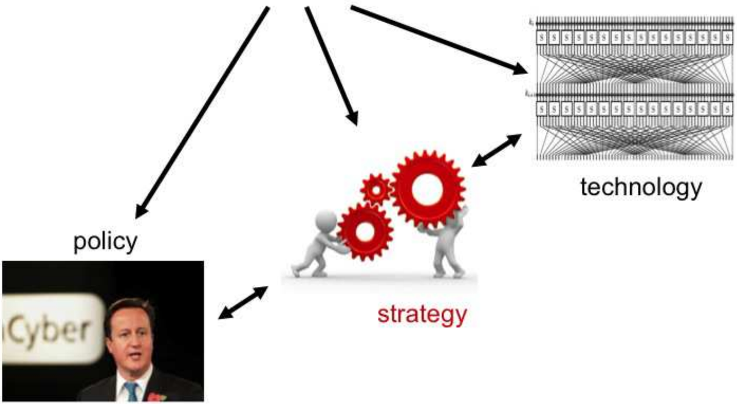
Politicians provide policies.

Cyber solutions



Technologists provide technologies.

Cyber solutions



Who provides the strategies?

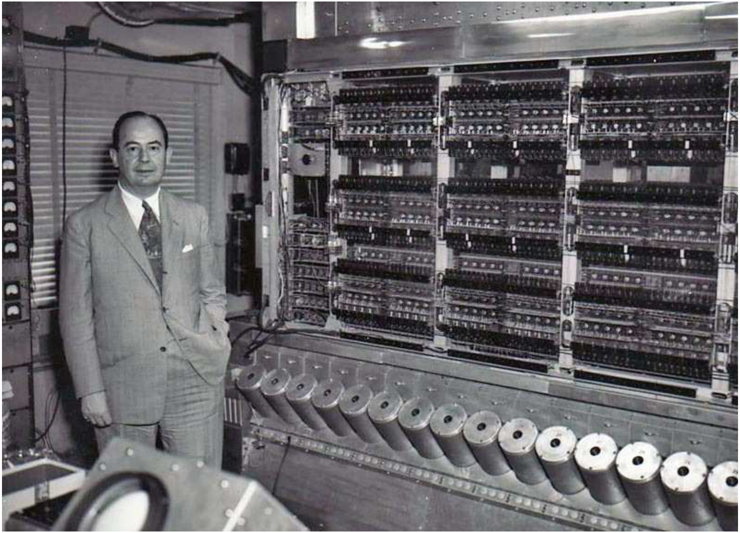
Queen's Strategysts

Men in the Middle of the Babington plot

Strategyst of Conflict

Science of politics as a state of conflict

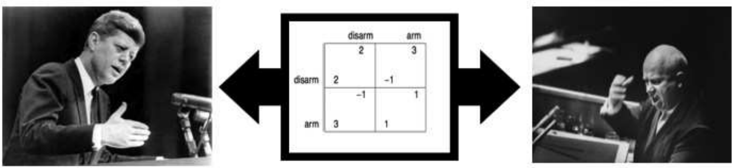
Compleat Strategyst



Strategy as a *mathematical* solution

One-shot conflict: **MAD**

(Mutual Assured Destruction)



Game theory in one slide

$$A\times X \xrightarrow{\;u_k\;} \mathbb{R}$$

$$A_{-k}\times X \xrightarrow{\;BR_k\;} A_k$$

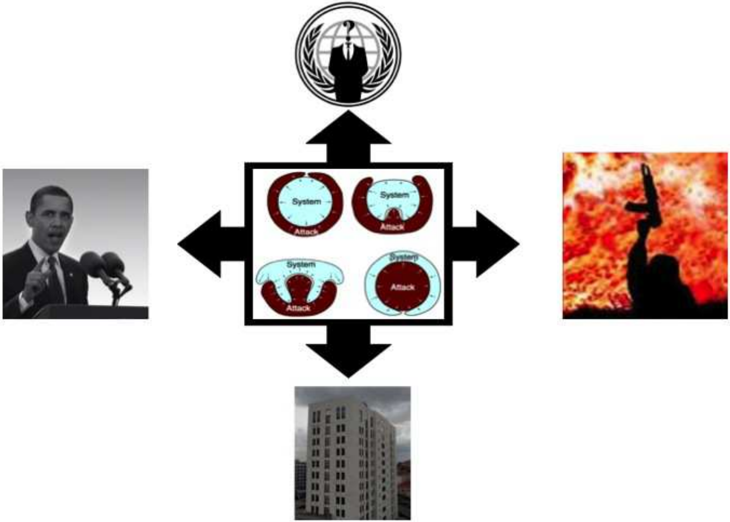
$$A\times X \xrightarrow{\;BR=\langle BR_k\circ\pi_k\rangle_{i=1}^{n}\;} A$$

$$\begin{array}{ccc} X & \xrightarrow{\;\;NE\;\;} & A \\ & {\scriptstyle NE}\searrow \quad \nearrow{\scriptstyle BR} & \\ & A & \end{array}$$

where

$$A=\prod_{i\in n} A_i \qquad X=\prod_{i\in n} X_i \qquad A_{-i}=\prod_{\substack{k\in n\\ k\neq i}} A_k$$

Ongoing conflict: **APT**
(Advanced Persistent Threat)



Ongoing conflict: **APT**

(Advanced Persistent Threat)

Obvious idea

- Security is an adversarial process.
- Game theory is the theory of adversarial processes.

$\Rightarrow$ Model security as a game!

Why is this not done already?

- Economists use game theory daily.
- Why not security engineers?

A possible reason

- Game theory tells you how to win following the rules
  - the rules are assumed to be enforced
  - the players follow the rules
- Security is the problem of enforcing the rules
  - the defender sets and implements the rules
  - the attacker seeks to cheat and defy the rules

A possible reason

- Game theory tells you how to win following the rules
  - the rules are assumed to be enforced
  - the players follow the rules
- Security is the problem of enforcing the rules
  - the defender sets and implements the rules
  - the attacker seeks to cheat and defy the rules

Game theory begins where security ends.

Security is a **hyper** game

- rules keep changing
- strategies keep adapting

Task

Develop a *"hyper game theory"* .

Task

Develop a method to evolve *adaptive strategies*.

Question

- Why is attack easier than defense?

Question

- Why is attack easier than defense?
- Why are attackers more adaptive than defenders?

Outline

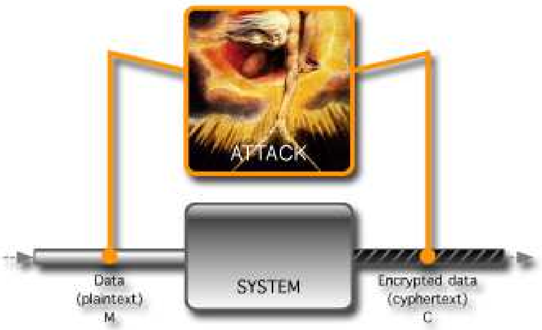
Problem: Strategic bias

Background: Attacker models

Approach: Learning strategies

Summary

Shannon's attacker: computationally unbounded
(omnipotent computer)

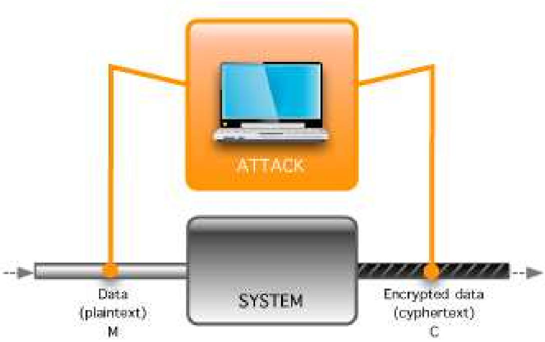


If a source contains some information,
then the attack will extract that information.

Shannon's attacker: computationally unbounded
(omnipotent computer)

$$\mathsf{Adv}_{\mathsf{E}}^{Sh} = \int_{m \leftarrow \mathsf{M}} \Pr\left(m \leftarrow \mathsf{M} \mid c = \mathsf{E}(m)\right) - \Pr\left(m \leftarrow \mathsf{M}\right)$$

Diffie-Hellman's attacker: computationally bounded
(real computer)



If attacker's computers have limited powers, then information can be hard to extract.

Diffie-Hellman's attacker: computationally bounded

(real computer)

$$\mathrm{Adv}_{\mathsf{E}}^{DH}(\mathsf{A}) \;=\; \Pr\big(m \leftarrow \mathsf{A}(c) \mid c = \mathsf{E}(m)\big) \;-\; \Pr\big(m \leftarrow \mathsf{A}(0)\big)$$

Diffie-Hellman's attacker: computationally bounded
(real computer)

$$\mathsf{Adv}^{DH}_{\mathsf{E}}(\mathsf{A}) \;=\; \Pr\Big(m \leftarrow \mathsf{A}(c) \mid c = \mathsf{E}(m)\Big) - \Pr\Big(m \leftarrow \mathsf{A}(0)\Big)$$

$$\mathsf{Adv}^{DH}_{\mathsf{E}} \;=\; \bigvee_{\mathsf{A}\in PPT} \mathsf{Adv}^{DH}_{\mathsf{E}}(\mathsf{A})$$

Diffie-Hellman's attacker: computationally bounded

(real computer)

Idea

$\mathrm{Adv}_{\mathsf{E}}^{DH} \sim 0$ iff E is a *one-way function*, i.e. for almost all m holds

$$\begin{aligned} \exists k.\ D\big(m, \mathsf{E}(m)\big) &\leq \mathcal{O}\big(\ell(m)^k\big) \\ \forall k.\ D\big(\mathsf{E}(m), m\big) &> \mathcal{O}\big(\ell(m)^k\big) \end{aligned}$$

where for ensembles a, b we define

$$D(a,b) = \bigwedge_{\{p\}(a)=b} time(p,a)$$

Adaptive attacker: computationally bounded
(real computer)

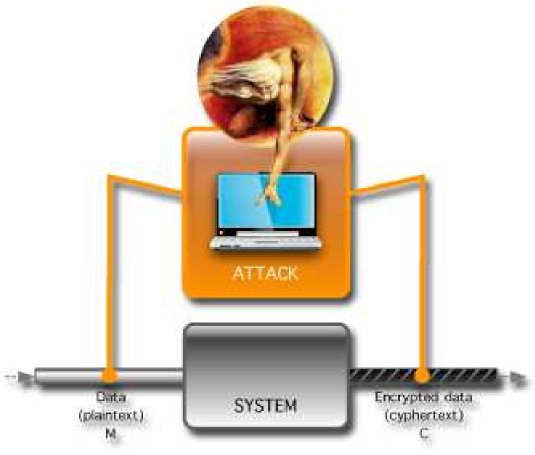
$$\mathrm{Adv}_s^{IND-CCA2}(\mathsf{A}) \quad =$$

$$\Pr\left(b \leftarrow \mathsf{A}_3\left({}^{\bullet}m,\ {}^{\bullet}c, \sigma_2, c_?, m_1, m_0, m^{\bullet}, c^{\bullet}\right)\ \middle|\ \begin{array}{r} {}^{\bullet}m = \mathsf{D}_s\left(\overline{k},\ {}^{\bullet}c\right), \langle {}^{\bullet}c_{\neq c_?}, \sigma_2\rangle \leftarrow \mathsf{A}_2(c_?, m_1, m_0, \sigma_1, m^{\bullet}, c^{\bullet}) \\ c_? \leftarrow \mathsf{E}_s(k, m_b), b \leftarrow U_2, \langle m_1, m_0, \sigma_1\rangle \leftarrow \mathsf{A}_1(m^{\bullet}, c^{\bullet}, \sigma_0), \\ m^{\bullet} = \mathsf{D}_s(\overline{k}, c^{\bullet}), \langle c^{\bullet}, \sigma_0\rangle \leftarrow \mathsf{A}_0 \end{array}\right)$$

$$- \quad \Pr\left(b \leftarrow U_2\right)$$

Kerckhoffs' attacker: logically unbounded

(real computer, omnipotent programmer)



...but if there is a feasible attack algorithm,
then attacker's omnipotent programmers will find it.

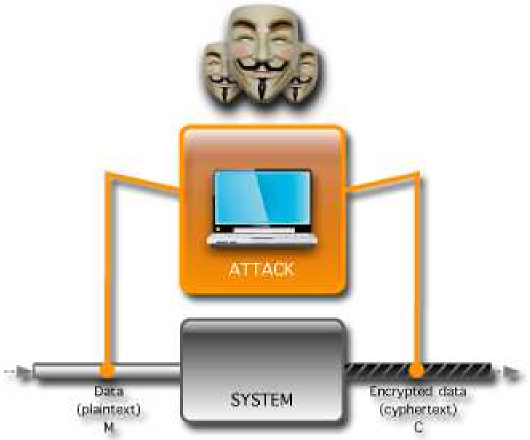
Kerckhoffs' attacker: logically unbounded

(real computer, omnipotent programmer)

$$
\begin{aligned}
\mathrm{Adv}_s^{IND-CCA2} \; = \\
\bigvee_{A \in PPT} \; \Pr\Big(b \leftarrow A_3\left({}^\bullet m,\ {}^\bullet c, \sigma_2, c_?, m_1, m_0, m^\bullet, c^\bullet\right) \;\Big| \\
{}^\bullet m = D_s\left(\overline{k},\ {}^\bullet c\right), \langle {}^\bullet c_{\neq c_?}, \sigma_2\rangle \leftarrow A_2(c_?, m_1, m_0, \sigma_1, m^\bullet, c^\bullet) \\
c_? \leftarrow E_s(k, m_b), b \leftarrow U_2, \langle m_1, m_0, \sigma_1\rangle \leftarrow A_1(m^\bullet, c^\bullet, \sigma_0), \\
m^\bullet = D_s(\overline{k}, c^\bullet), \langle c^\bullet, \sigma_0\rangle \leftarrow A_0 \Big) \\
- \; \Pr\Big(b \leftarrow U_2\Big)
\end{aligned}
$$

ASECO attacker: logically bounded

(real computer, **real** programmer)



If attacker's programmers have limited powers,
then attack algorithms may be hard to find.

ASECO attacker: logically bounded

(real computer, **real** programmer)

$$\mathrm{Adv}_{s}^{IND-ASECO}(\mathbb{A}) \quad = $$

$$\bigvee_{a \leftarrow \mathbb{A}(s)} \Pr\Big(b \leftarrow \{a_3\}({}^\bullet m,\ {}^\bullet c, c_?, m_1, m_0, m^\bullet, c^\bullet)\ \Big|$$

$$ {}^\bullet m = \{d_s\}\big(\overline{k},\ {}^\bullet c\big), {}^\bullet c \leftarrow \{a_2\}(c_?, m_1, m_0, m^\bullet, c^\bullet)$$

$$c_? \leftarrow \{e_s\}(k, m_b), b \leftarrow U_2, \langle m_1, m_0\rangle \leftarrow \{a_1\}(m^\bullet, c^\bullet),$$

$$m^\bullet = \{d_s\}(\overline{k}, c^\bullet), c^\bullet \leftarrow \{a_0\}\Big)$$

$$- \quad \Pr\Big(b \leftarrow U_2\Big)$$

Adaptive security game

(both attacker and defender have real computers and real programmers)

$$\mathrm{Adv}^{IND-ASECO}(\mathbb{A}, \mathbb{S}) \quad =$$

$$\bigwedge_{s \leftarrow \mathbb{S}(a)} \quad \bigvee_{a \leftarrow \mathbb{A}(s)} \Pr\left(b \leftarrow \left\{a_3\right\}({}^{\bullet}m,\ {}^{\bullet}c, \ldots) \;\middle|\; \begin{array}{r} {}^{\bullet}m = \left\{d_s\right\}\left(\overline{k},\ {}^{\bullet}c\right), {}^{\bullet}c \leftarrow \left\{a_2\right\}(c_?, m_1, m_0, m^{\bullet}, c^{\bullet}) \\ c_? \leftarrow \left\{e_s\right\}(k, m_b), b \leftarrow U_2, \langle m_1, m_0 \rangle \leftarrow \left\{a_1\right\}(m^{\bullet}, c^{\bullet}), \\ m^{\bullet} = \left\{d_s\right\}(\overline{k}, c^{\bullet}), c^{\bullet} \leftarrow \left\{a_0\right\} \end{array} \right)$$

$$- \quad \Pr\left(b \leftarrow U_2 \right)$$

Adaptive security game

(both attacker and defender have real computers and real programmers)

Idea

$\mathsf{Adv}_{E}^{IND-ASECO}(\mathbb{A},\mathbb{S}) \sim 0$ iff for $a \leftarrow \mathbb{A}(s)$ and $s \leftarrow \mathbb{S}(a)$ holds with overwhelming probability

$$\begin{aligned} \exists k.\ D\big(a,s\big) & \leq & \mathcal{O}\big(\ell(a)^k\big) \\ \forall k.\ D\big(s,a\big) & > & \mathcal{O}\big(\ell(s)^k\big) \end{aligned}$$

where

$$D(a,b) = \bigwedge_{\{p\}(a)=b} time(p,a)$$

Adaptive security game

(both attacker and defender have real computers and real programmers)

Idea

$\text{Adv}_{E}^{IND-ASECO}(\mathbb{A}, \mathbb{S}) \sim 0$ iff for $a \leftarrow \mathbb{A}(s)$ and $s \leftarrow \mathbb{S}(a)$ holds with overwhelming probability

$$\begin{aligned} \exists k.\ D\big(a, s\big) &\leq \mathcal{O}\big(\ell(a)^k\big) \\ \forall k.\ D\big(s, a\big) &> \mathcal{O}\big(\ell(s)^k\big) \end{aligned}$$

where

$$D(a, b) = \bigwedge_{\{p\}(a)=b} time(p, a)$$

...with a couple of tweaks.

Summary: Beyond omnipotence

power	*unbounded*	*bounded*
rationality	Cournot	Simon
computational	Shannon	Diffie-Hellman
logical	Kerckhoffs	ASECO

Outline

Problem: Strategic bias

Background: Attacker models

Approach: Learning strategies

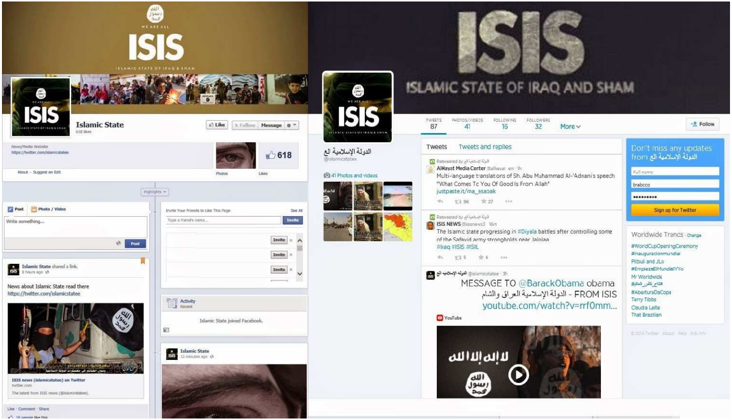
Strategic bias beyond cryptography

Game of attack vectors

Modeling adaptive games

Summary

Beyond crypto: A real adaptive attacker



recruits his fighters using defender's networks

Beyond crypto: A real adaptive attacker

buys his weapons on defender's free market

Beyond crypto: A real adaptive attacker

makes cyber war physical!

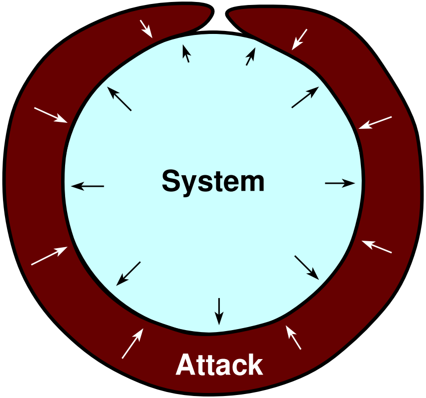
Question

- When is a defense strategy adaptive?

Question

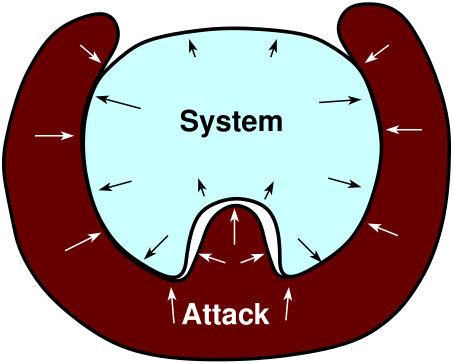
- When is a defense strategy adaptive?
- When is intelligence adaptive?

Game of attack vectors: **Fortification**



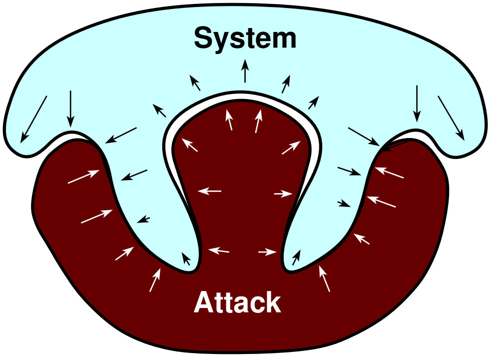
System must defend all vectors, Attacker just needs one

Game of attack vectors: **Honeypot**



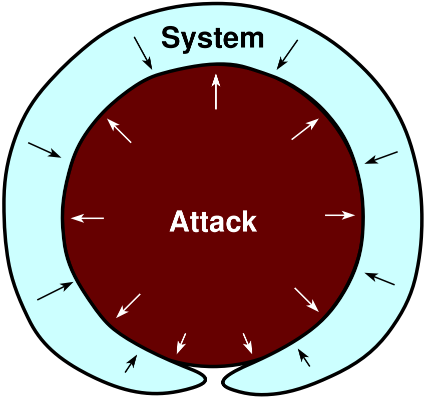
System passively observes Attacker

Game of attack vectors: **Sampling**



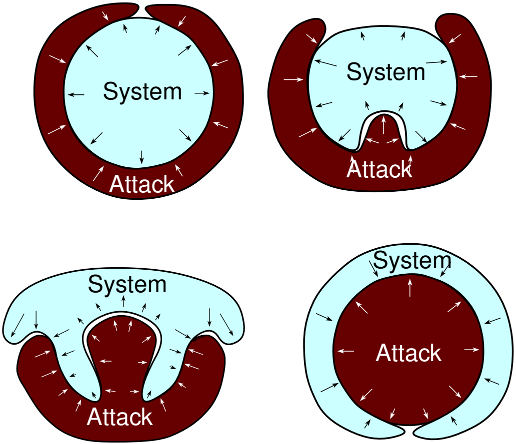
System actively queries Attacker

Game of attack vectors: **Adaptation**



Attacker must defend all markers, System just needs one

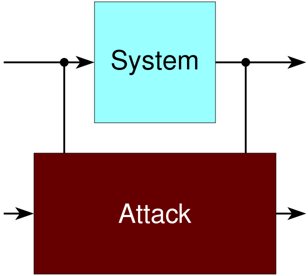
From fortification to adaptation



Fortress under siege evolves into macrophage devouring a bacterium

From fortification to adaptation in Crypto

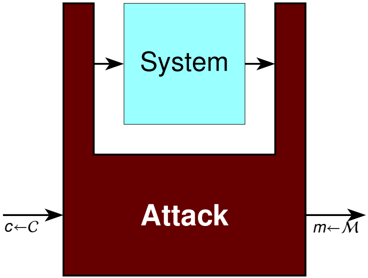
Passive attacker



observes plaintext/ciphertext pairs

From fortification to adaptation in Crypto

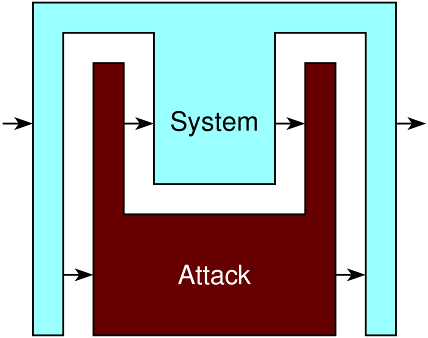
Adaptive attacker



queries System by chosen plaintexts and/or ciphertexts

From fortification to adaptation in Crypto

Adaptive defender



"Answer questions by questions"

From fortification to adaptation beyond Crypto

Security analysis strategy

- The world consists Good Guys and Bad Guys.
- Analyst profiles and detects Bad Guys.
- Defender keeps Good Guys in and Bad Guys out.

From fortification to adaptation beyond Crypto

Security analysis strategy

- The world consists Good Guys and Bad Guys.
- Analyst profiles and detects Bad Guys.
- Defender keeps Good Guys in and Bad Guys out.
- Problem: false positives and false negatives

From fortification to adaptation beyond Crypto

Sponsored search strategy

- The world consists of Buyers with various interests.
- Analyst profiles and quantifies Buyers' interests.
- Offers triggered through *significance testing*

From fortification to adaptation beyond Crypto

Sponsored search strategy

- The world consists of Buyers with various interests.
- Analyst profiles and quantifies Buyers' interests.
- Offers triggered through *significance testing*
- Advertiser influences the interests.

From fortification to adaptation beyond Crypto

Adaptive analysis strategy

- The world consists of Guys with various interests.
- Analyst profiles and quantifies Guys' interests.
- Defense triggered through *significance testing*.

From fortification to adaptation beyond Crypto

Adaptive analysis strategy

- The world consists of Guys with various interests.
- Analyst profiles and quantifies Guys' interests.
- Defense triggered through *significance testing*.
  - False positives are kept below the threshold
  - Interests can be influenced

From fortification to adaptation beyond Crypto

Adaptive analysis strategy

- The world consists of Guys with various interests.
- Analyst profiles and quantifies Guys' interests.
- Defense triggered through *significance testing*.
  - False positives are kept below the threshold
  - Interests can be influenced

(∼ *"Towards a science of trust"*)

Category of strategies

Definition

Let $\mathcal{C}$ be a cartesian category, and $\Delta : \mathcal{C} \longrightarrow \mathcal{C}$ a commutative monad over it.

The category $\mathcal{S} = \mathcal{S}_{\Delta\mathcal{C}}$ of Δ-strategies over $\mathcal{C}$ consists of

- players $A = \langle M_A, S_A \rangle \in \mathcal{C}^2$
- strategies $(A \xrightarrow{\Phi} B) \in \mathcal{C}\big(M_A \times S_B,\ \Delta(S_B \times M_B)\big)$

Category of strategies

Composition

$$\frac{A \xrightarrow{\Phi} B \qquad\qquad B \xrightarrow{\Psi} C}{A \xrightarrow{\Phi;\Psi} C}$$

is given by

$$(\Phi;\Psi)_{a\gamma\gamma' c} \quad = \quad \sum_{\beta\beta' b} \Phi_{a\beta\beta' b} \cdot \Psi_{b\gamma\gamma' c}$$

Games of perfect and complete information

$$S_A \;=\; S_B \;=\; (\mathbb{R} \times \mathbb{R})^{M_A \times M_B}$$

Best Response strategies

$$\langle b, \sigma^A \rangle \xrightarrow{\Sigma_A} \langle \sigma^A, a \rangle \iff \forall x \in M_A.\ \sigma^A_{xb} \leq \sigma^A_{ab}$$

$$\langle a, \sigma^B \rangle \xrightarrow{\Sigma_B} \langle \sigma^B, b \rangle \iff \forall y \in M_B.\ \sigma^B_{ay} \leq \sigma^B_{ab}$$

Nash equilibrium

$$\dfrac{\dfrac{A \xrightarrow{\Sigma_B} B \qquad\qquad B \xrightarrow{\Sigma_A} A}{A \xrightarrow{\Sigma_B;\Sigma_A} A \qquad\qquad B \xrightarrow{\Sigma_A;\Sigma_B} B}}{\begin{array}{ccc} 1 & \xrightarrow{\quad NE \quad} & A \times B \\ & {\scriptstyle NE}\searrow \qquad \nearrow{\scriptstyle (\Sigma_B;\Sigma_A)\times(\Sigma_A;\Sigma_B)} & \\ & A \times B & \end{array}}$$

Games of imperfect and complete information

$$S_A = P_A \times (\mathbb{R} \times \mathbb{R})^{M_A \times M_B}$$
$$S_B = P_B \times (\mathbb{R} \times \mathbb{R})^{M_A \times M_B}$$

Games of perfect and incomplete information

$$
\begin{aligned}
S_A &= \mathbb{R}^{M_A \times M_B} \times \Delta S_B \\
S_B &= \mathbb{R}^{M_A \times M_B} \times \Delta S_A
\end{aligned}
$$

Games of perfect and incomplete information

$$S_A = S_B = \prod_{i=0}^{\infty} \Delta^i \left(\mathbb{R}^{M_A \times M_B}\right)$$

Outline

Problem: Strategic bias

Background: Attacker models

Approach: Learning strategies

Summary

Strategic paradigms

System security

"The security policy must be explicit, well defined and enforced by the computer."

Orange Book (1983-2002)

Adaptive security

"Let your methods be guided by the infinite variety of circumstances."

Sun Tzu (544 BC - 496 BC)

Strategic paradigms

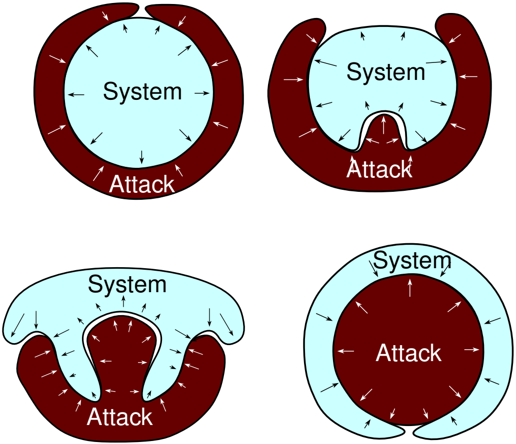
System security

- "no security by obscurity"
- "precise attacker model"

Adaptive security

- "be mysterious"
- "opportunities multiply"

From fortification to adaptation



Fortress under siege evolves into
macrophage devouring a bacterium

It is good to keep the invaders out. . .

. . . but it is better to bring them in